THE METAPHOR IS THE KEY: CRYPTOGRAPHY, THE CLIPPER CHIP, AND THE CONSTITUTION

A. MICHAEL FROOMKIN†

TABLE OF CONTENTS

---

† © A. Michael Froomkin, 1995. Associate Professor, University of Miami School of Law. B.A. 1982, Yale College; M.Phil. 1984, Cambridge University; J.D. 1987, Yale Law School. Internet: Mfroomki@Umiami.ir.miami.edu (PGP 2.6.2 public key appears *infra* note 787). Research for this article was supported by the University of Miami School of Law Summer Research Grant Fund. SueAnn Campbell, Nora de la Garza, Yolanda Jones, and Brian Williams provided superb library support, Rosalia Lliraldi provided secretarial support, and Julie Owen provided indefatigable research assistance. I am grateful to Abe Abraham, Stewart Baker, Tom Baker, Ken Bass, Caroline Bradley, Dorothy Denning, John Ely, Steve Fishbein, John Gilmore, Lance Hoffman, Mark Lemly, Larry Lessig, Charles C. Marson, George Mundstock, David Post, Jonathan Simon, Miles Smid, David Sobel, Cleveland Thorton, Lee Tien, Eugene Volokh, Stephen F. Williams, Steve Winter, two anonymous bureaucrats, and the participants in a University of Miami faculty seminar for their comments, corrections, and suggestions. I first encountered several of the issues discussed in this Article in the Cypherpunks and Cyberia-L mailing lists, and on the misc.legal.moderated newsgroup. For an earlier version of portions of Part III of this Article, see A. Michael Froomkin, *The Constitutionality of Mandatory Key Escrow–A First Look, in* BUILDING IN BIG BROTHER: THE CRYPTOGRAPHIC POLICY DEBATE (Lance Hoffman ed., forthcoming Mar. 1995) (manuscript at 413) [hereinafter BUILDING IN BIG BROTHER].

Unless otherwise specified, this Article reflects legal and technical developments occurring on or before January 1, 1995.

INTRODUCTION

> Without the ability to keep secrets, individuals lose the capacity to distinguish themselves from others, to maintain independent lives, to be complete and autonomous persons. . . . This does not mean that a person actually has to keep secrets to be autonomous, just that she must possess the *ability* to do so. The ability to keep secrets implies the ability to disclose secrets selectively, and so the capacity for selective disclosure at one's own discretion is important to individual autonomy as well.[1]

Secrecy is a form of power.[2] The ability to protect a secret, to preserve one's privacy, is a form of power.[3] The ability to penetrate secrets, to learn them, to use them, is also a form of power. Secrecy empowers, secrecy protects, secrecy hurts. The ability to learn a person's secrets without her knowledge—to pierce a person's privacy in secret—is a greater power still.

People keep secrets for good reasons and for evil ones. Learning either type of secret gives an intruder power over another. Depending on the people compromised and the secrets learned, this power may be deployed for good (preventing a planned harm) or ill (blackmail, intimidation).

This Article is about the clash between two types of power: the individual's power to keep a secret from the state and others, and the state's power to penetrate that secret.[4] It focuses on new

---

[1] KIM L. SCHEPPELE, LEGAL SECRETS 302 (1988) (footnote omitted).

[2] "Secrecy" refers to the intentional concealment of information so as to prevent others from "possessing it, making use of it, or revealing it" to third parties. SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 6 (1982). It also refers to "the methods used to conceal [information], such as codes or disguises." *Id.*

[3] Privacy is "that portion of human experience for which secrecy is regarded as most indispensable." *Id.* at 7. Secrecy and privacy are not identical, however. *See id.* at 10. Privacy is "the condition of being protected from unwanted access by others—either physical access, personal information, or attention. Claims to privacy are claims to control access to what one takes . . . to be one's personal domain." *Id.* at 10-11.

[4] In this sense, "the right to privacy has everything to do with delineating the legitimate limits of governmental power." Jed Rubenfeld, *The Right of Privacy*, 102

conflicts between the perennial desire of law enforcement and intelligence agencies to have the capability to penetrate secrets at will, and private citizens who are acquiring the ability to frustrate these desires. This is an article about the Constitution and the arcana of secret-keeping: cryptography.[5]

This is also a long article. It is long because it addresses three complex issues. First, it outlines some of the promises and dangers of encryption. Second, it analyzes the constitutional implications of a major government proposal premised on the theory that it is reasonable for the government to request (and perhaps some day to require) private persons to communicate in a manner that makes governmental interception practical and preferably easy. Third, it speculates as to how the legal vacuum regarding encryption in cyberspace shortly will be, or should be, filled.

What fills that vacuum will have important consequences. The resolution of the law's encounter with cryptography has implications far beyond whether the government adopts the Clipper Chip or whether a particular cipher may be licensed for export. The resolution of this debate will shape the legal regulation of cyberspace and in so doing shape its social structures and social ethics.

Cryptologists[6] use a few terms that may not be familiar to lawyers, and it is useful to define them at the outset of any discussion relating to encryption. *Cryptography* is the art of creating and using methods of disguising messages, using codes, ciphers, and other methods, so that only certain people can see the real message. Codes and ciphers are not the same. A *code* is a system of communication that relies on a pre-arranged mapping of meanings such as those found in a code book. A *cipher* is a method of encrypting any text regardless of its content.[7] Paul Revere's "[o]ne, if by land, and two, if by sea" was a code.[8] If the British had landed by parachute,

---

HARV. L. REV. 737, 737 (1989). Of course, true privacy also requires delineating the limits of the power of private parties, including detectives, credit bureaus, and others.

[5] Cryptography cuts across the law in many interesting ways. Most of the statutory issues, however, are outside the scope of this Article. In particular, this Article does not discuss cryptography as it relates to intellectual property law.

[6] *Cryptology* is the study of cryptography and cryptanalysis. *See* DAVID KAHN, THE CODEBREAKERS at xvi (1967).

[7] *See id.* at xiii-xvi; *see also* Horst Feistel, *Cryptography and Computer Privacy*, SCI. AM., May 1973, at 15, 15 (drawing a distinction between codes and ciphers).

[8] HENRY W. LONGFELLOW, *The Landlord's Tale: Paul Revere's Ride*, *in* 4 THE POETICAL WORKS OF HENRY WADSWORTH LONGFELLOW 25, 25 (1966). For an example of a literary cipher, see EDGAR A. POE, *The Gold-Bug*, *in* THE COMPLETE TALES AND POEMS OF EDGAR ALLAN POE 42, 62-67 (1938). *See also* Terence Whalen,

no quantity of lanterns would have sufficed to communicate the message. The modern cryptographic systems discussed in this Article are all ciphers, although some are also known as electronic code books.

Those who are supposed to be able to read the message disguised by the code or cipher are called *recipients*. "The original message is called a *plaintext*. The disguised message is called a *ciphertext*. *Encryption* means any procedure to convert plaintext into ciphertext. *Decryption* means any procedure to convert ciphertext into plaintext."[9] An *algorithm* is a more formal name for a cipher. An algorithm is a mathematical function used to encrypt and decrypt a message. Modern algorithms use a *key* to encrypt and decrypt messages.[10] A *single-key* system is one in which both sender and receiver use the same key to encrypt and decrypt messages. Until recently, all ciphers were single-key systems. One of the most important advances in cryptography is the recent invention of *public-key systems*, which are algorithms that encrypt messages with a key that permits decryption only by a different key.[11] The legal and social implications of this discovery figure prominently in this Article.

Cryptanalysis is the art of breaking the methods of disguise invented with cryptography. Lawyers will recognize the cryptographers' terms for cryptanalysts who seek to read messages intended only for recipients: *enemies*, *opponents*, *interlopers*, *eavesdroppers*, and *third parties*.[12] In this Article, however, cryptanalysts who work for U.S. law enforcement or intelligence organizations such as the FBI or the National Security Agency (NSA) will be called *public servants*. *Key escrow* refers to the practice of duplicating and holding the key to a cipher—or the means of recreating or accessing the key to a cipher—so that some third party (the escrow agent) can decrypt messages using that cipher. As used in the Clipper Chip debates, the term "escrow" is something of a misnomer because the escrow is

---

The Code for Gold: Edgar Allan Poe and Cryptography, 46 REPRESENTATIONS 35 (1994).

[9] Eric Bach et al., *Cryptography FAQ (03/10: Basic Cryptology)* § 3 (Oct. 31, 1994), *available online URL* ftp://rftm.mit.edu/pub/usenet/news.answers/cryptography-faq/part03. A message that has never been disguised is called a *cleartext*. *See* KAHN, *supra* note 6, at xvi.

[10] The number of possible values of a key is called the *keyspace*.

[11] *See infra* Technical Appendix, part B (describing public-key cryptography).

[12] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 4 (1994) (defining cryptanalytic terms).

primarily for the benefit of the government rather than the owner of the key.

Part I of this Article describes advances in encryption technology that are increasing personal privacy, particularly electronic privacy, but reducing the U.S. government's ability to wiretap telephones, read e-mail surreptitiously, and decrypt computer disks and other encrypted information. To ensure the continuation of the wiretapping and electronic espionage capabilities that it has enjoyed since soon after the invention of the telegraph and the telephone,[13] the government has devised an Escrowed Encryption Standard (EES),[14] to be implemented in the Clipper Chip[15] and other similar devices.[16] In Clipper and related products the government

---

[13] On the early use of telegraphic cryptography in military combat, see KAHN, *supra* note 6, at 190-91.

[14] *See* Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997, 5998 (1994) [hereinafter FIPS 185] ("Key escrow technology was developed to address the concern that widespread use of encryption makes lawfully authorized electronic surveillance difficult."). For a discussion of Federal Information Processing Standards (FIPS), see *infra* notes 222-25 and accompanying text.

[15] Although the chip is universally known as "Clipper," the government has alternately adopted and abandoned the name. *See* U.S. GEN. ACCOUNTING OFFICE, COMMUNICATIONS PRIVACY: FEDERAL POLICY AND ACTIONS 6 n.6 (1993) [hereinafter GAO COMMUNICATIONS PRIVACY] (explaining that the name was used, then dropped). The official use of the name "Clipper" recently has been revived. *See* SUSAN LANDAU ET AL., ASSOCIATION FOR COMPUTING MACHINERY, INC., CODES, KEYS AND CONFLICTS: ISSUES IN U.S. CRYPTO POLICY 52 n.1 (1994) [hereinafter ACM REPORT] (stating that Intergraph Corp., which had trademarked the name for one of its microprocessors, "graciously ceded" the rights to the name).

[16] The technical name for the Clipper-compliant family of devices is the Escrowed Encryption Standard (EES). For the nonclassified specifications for these devices, see FIPS 185, *supra* note 14, at 6004-05. The Clipper Chip itself is designed for use in secure telephones; its cousin, the Capstone Chip, will be used for electronic mail, digital signatures, *see infra* Technical Appendix, part C, public key exchange, *see infra* Technical Appendix, part B, and random number generation. For a brief introduction to the Capstone Chip and its technical specifications, see generally National Inst. of Standards and Technology, *Capstone Chip Technology* (Apr. 30, 1993), *in* BUILDING IN BIG BROTHER, *supra* note † (manuscript at 147) [hereinafter *Capstone Chip Technology*]. A PCMCIA card (Type 1) using Capstone will likely be purchased in bulk by the Pentagon. *See infra* text accompanying note 245. The PCMCIA card was formerly known as a "Tessera" card, but the National Institute of Standards and Technology (NIST) has now changed the name to the "Fortezza" card because a private company had previously trademarked the name "Tessera." *See* Interview with Gary Latham, Mantech Strategic Associates, Ltd., in Miami, Fla. (Sept. 30, 1994) (Mr. Latham is a consultant employed by NIST); *see also* Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, *in* BUILDING IN BIG BROTHER, *supra* note † (manuscript at 131, 145) (noting that "Tessera" is a trademark of Tessera, Inc., which has no connection with the EES project).

proposes a simple bargain: In exchange for providing the private sector with an encryption technology certified as unbreakable for years to come by the NSA,[17] the government plans to keep a copy of the keys[18]—the codes belonging to each chip—which, the government hopes, will allow it to retain the ability to intercept messages sent by the chip's user. The government's proposal includes procedures designed to reduce the risk that the keys would be released to law enforcement agencies without legally sufficient justification, although the likely effectiveness of these procedures is debatable. Most U.S. residents remain free, however, to reject the government's offer, use alternatives to Clipper (so long as the software or hardware remains in the U.S.),[19] and withhold their keys from the government.[20] With ever more secure methods of

---

The entire EES project has been plagued by problems with intellectual property law. Not only did the names originally selected for the EES chips conflict with existing trademarks, but the algorithm for the escrow concept itself was the subject of an infringement claim by MIT professor Silvio Micali. Professor Micali claimed he had patented the escrow concept. After initially denying there was infringement, NIST agreed to settle Professor Micali's claim by purchasing a nonexclusive license for all EES systems "developed for authorized government law enforcement purposes" whether inside or outside the government. U.S. Dep't of Commerce, Patent Agreement Removes Perceived Barrier to Telecommunications Security System (July 11, 1994) (press release); *see also* Ellen Messmer, *NIST Acknowledges Patent Infringement*, NETWORK WORLD, July 25, 1994, at 20 (noting that the exact terms of the NIST settlement agreement were not being revealed).

[17] Established in 1952 by presidential directive, the NSA is the U.S. government's chief signals intelligence and cryptological department. *See* KAHN, *supra* note 6, at 675-84 (outlining the development of the NSA from 1952 through 1966); JEFFREY RICHELSON, THE U.S. INTELLIGENCE COMMUNITY 15-20 (1985) (describing the bureaucratic structure of the NSA). *See generally* JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY (1982) (tracing the development of the NSA between 1952 and 1982).

[18] Vice President Gore has suggested that the proposal might be modified in the future to allow some companies to use certified private escrow agents rather than depositing their keys directly with the government. *See* Letter from Vice President Al Gore to Congresswoman Maria Cantwell (July 20, 1994), *available online URL* ftp://ftp.eff.org/pub/EFF/Policy/Crypto/Clipper/gore_clipper_retreat_cantwell_072094.letter [hereinafter Gore-Cantwell Letter]. *But see* Statement of Patrick Leahy on Vice President Gore's Clipper Chip Letter (July 21, 1994), *available online URL* ftp://ftp.eff.org/pub/EFF/Policy/Crypto/Clipper/gore_clipper_retreat_leahy.statement (stating that the Gore letter "represents no change in policy").

NIST is currently exploring alternatives to the existing EES proposal that would rely more heavily on third-party escrow agents. *See* Interview with Gary Latham, *supra* note 16.

[19] *See infra* part I.C.1.c.i (discussing the International Traffic in Arms Regulations (ITAR), which restrict the export of cryptographic software).

[20] The government can require that federal agencies and government contractors use Clipper. Indeed, the government has announced that the Attorney General will

encryption becoming easier to use, U.S. residents can protect their electronic communications and records so well that they are able to frustrate interception attempts by even the most sophisticated government agencies.[21]

Part II examines the legal justifications and constitutional implications of the EES proposal. It argues that the EES proposal violates the spirit, although not the letter, of the Administrative Procedures Act and represents an abuse of the technical standard-setting process. The involvement of the NSA may violate the Computer Security Act, but the absence of public information as to its role makes a firm judgment impossible. Part II also discusses Clipper's inherent policy and technical weaknesses and the inconsistencies between the Administration's policy objectives—to the extent they are unclassified—and the Clipper proposal itself. It concludes, however, that a purely voluntary Clipper program violates no statutory or constitutional provisions, and that even if it does, there is no one with standing to challenge such a violation. Part II also concludes that an optional Clipper will probably make only a modest contribution to the government's stated goal of maintaining its wiretap and electronic espionage capability.

Thus, Part III considers the constitutional implications of the more radical proposal that some commentators find implicit in the policies animating Clipper: requiring all users of strong encryption to register their ciphers' keys with the government. After a whirlwind survey of evolving conceptions of the constitutional right to privacy as well as more settled First, Fourth, and Fifth Amendment doctrines, Part III concludes that although mandatory key escrow would infringe personal privacy, reduce associational

---

purchase "several thousand" Clipper-equipped telephones. *See* Office of the Press Secretary, The White House, Statement by the Press Secretary 2 (Apr. 16, 1993), *in* Office of the Press Secretary, The White House, Government-Developed "Key Escrow" Chip Information Packet (Apr. 16, 1993) (information packet accompanying press release) [hereinafter "Key Escrow" Information Packet].

If Clipper becomes the exclusive encryption protocol used by the U.S. government, then anyone who wishes to communicate with the government concerning nonclassified but sensitive information will have to use Clipper.

[21] Without access to relevant classified information, it is impossible to know whether the NSA or other government agencies might have discovered a means of breaking even the most sophisticated publicly available ciphers. Considering the intense secrecy that would surround such a cryptanalytic capability, however, one can safely act as if it does not exist. Even if the government had the capability to break supposedly unbreakable cryptography, such cryptanalysis would be a vital national secret—so vital that the government would never use that capability in a manner that would risk revealing its existence before the middle of the next large war.

freedoms, potentially chill speech, constitute a potentially unreasonable search, and might even require a form of self-incrimination, the constitutionality of mandatory key escrow legislation remains a distressingly close question under existing doctrines.

Part IV addresses the cryptography controversy as an example of the law's occasionally awkward response to a new technology. The courts, and to a lesser extent the legislative and executive branches, have yet to come to grips with many cryptographic conundrums. As a result, this part of the legal "landscape" remains relatively barren. As more and more settlers arrive in cyberspace, the nature of this new landscape will depend critically on the legal metaphors that the colonists choose to bring with them.

Finally, the Technical Appendix discusses modern cryptographic systems, including the widely-used Data Encryption Standard (DES), and how they can (at least theoretically) be broken by attackers armed with large numbers of relatively modest computers. It also provides an introduction to public-key cryptosystems and to digital signatures, which could represent the most important commercial application of modern cryptographic techniques.

I. MODERN CRYPTOGRAPHY: PRIVATE SECURITY, GOVERNMENT INSECURITY

Cryptography contributes to commercial, political, and personal life in a surprising number of ways. Now that modern cryptographic techniques have put strong, perhaps uncrackable, cryptography within the reach of anyone with a computer or even a telephone, the use of strong cryptography is likely to increase further. As a result, worried law enforcement and intelligence agencies have developed the Clipper Chip in order to retain their capability to eavesdrop on private electronic communications.

A. *Who Needs Cryptography?*

Many individuals and businesses want or need communications and data security.[22] Although these desires clearly have an objective

---

[22] Cryptography remains of paramount importance in guarding military and other national-security-related secrets during both peacetime and wartime. These uses of cryptography are outside the scope of this Article, although it bears mentioning that to date the government remains by far the largest producer and consumer of cryptography in this country. *See* ACM REPORT, *supra* note 15, at 12 (noting that the private market for cryptography remains a niche market in which a handful of companies gross only a few tens of millions of dollars annually).

basis in many cases, some of these desires are undoubtedly symbolic and psychological. Who other than the recipient, after all, is likely to want to read most private faxes and e-mail?[23] The subjective nature of a desire for privacy makes it no less real or worthy of respect.[24] Encryption can play a critical role in contrib-uting to this communications and data security.[25]

The government's assurance that a cryptosystem is secure also contributes to this security. Evaluating the strength of a cipher is a black art that requires skills few businesses or individuals possess. The government's endorsement will at least reassure those, such as banks and lawyers, who have a duty to secure their communications and data but lack the technical knowledge to determine what ciphers are reliable.

1. Banks, ATM-Users, Electronic Transactors

Encryption is heavily used in banking, both in the United States and abroad. Fedwire and the Clearing House Interbank Payment System process a daily total of more than 350,000 messages with an estimated value of between $1 and $2 trillion. These transactions rely on U.S. government-approved encryption to protect against unauthorized modification and forgery.[26] The U.S. Department of the Treasury requires encryption of all U.S. electronic funds transfer

---

[23] *But see infra* part I.C.1.b (discussing the NSA's traffic analysis); *infra* note 405 and accompanying text (discussing the use of voice recognition as a surveillance tool).

[24] *See, e.g.*, SCHEPPELE, *supra* note 1, at 302 (commenting on the importance of secrecy at the individual level).

[25] Of course, cryptography will not protect against all breaches of security. There are many other ways to lose one's privacy, including trusting the wrong people, leaving things in plain sight, and, of course, simple stupidity. Electronic listening devices also make people vulnerable. *See, e.g.*, Kent Greenfield, Comment, *Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment*, 58 U. CHI. L. REV. 1045, 1047-48 (1991) (describing miniature video cameras and other surveillance technologies); *see also High-Tech Tools for Police Will "See Through" Clothes*, INT'L HERALD TRIB., Dec. 19, 1994, at 4 (reporting that police may soon carry electromagnetic wave imagers that detect guns concealed under clothing).

[26] *See* Gilles Garon & Richard Outerbridge, *DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990s*, CRYPTOLOGIA, July 1991, at 177, 177 (stating that since its adoption in 1977, DES "has become the most widely used cryptographic system in the world"); Lance J. Hoffman et al., *Cryptography Policy*, COMM. ACM, Sept. 1994, at 109, 111 (noting that the Clearing House Interbank payment system currently moves an average of $1 trillion each day via wire and satellite). Both systems use the U.S. Data Encryption Standard (DES), which arguably has reached or will soon reach the end of its useful life for high-value security. *See infra* part I.B (noting that existing methods of encryption are beginning to look dated and vulnerable).

messages.[27]

Banks use encryption to protect ID numbers that customers use at bank automated teller machines (ATMs).[28] In addition, many banks encrypt the customer data on ATM cards in order to protect against forgeries.[29] The banking sector's awareness of its vulnerability to electronic theft of funds has spurred the creation of cryptographic standards for both retail and inter-bank transactions.[30]

As the economy continues to move away from cash transactions towards "digital cash," both customers and merchants will need the authentication provided by unforgeable digital signatures in order to prevent forgery and transact with confidence.[31] Forgery is a perennial problem with electronic mail: copying is easy, there are no tangible permanent media involved in the communication, and programmers or system managers can alter e-mail headers to fake the source of a message. Cryptography can provide an authenticating function for these electronic transactions. Cryptographic

---

[27] *See* Gerald Murphy, U.S. Dep't of the Treasury, Directive: Electronic Funds and Securities Transfer Policy–Message Authentication and Enhanced Security, No. 16-02, § 3 (Dec. 21, 1992).

[28] *See* AMERICAN NAT'L STANDARDS COMMITTEE ON FINANCIAL SERVICES, X9 SECRETARIAT, AMERICAN BANKERS ASS'N, AMERICAN NATIONAL STANDARD FOR PERSONAL IDENTIFICATION NUMBER (PIN) MANAGEMENT AND SECURITY 9 (1982) (describing proper ATM encryption standards); *see also* Beth E. Secaur, Note, *Automated Teller Machines Under the New York Banking Law: Do They Serve Community Credit Needs?*, 37 SYRACUSE L. REV. 117, 120-23 (1986) (discussing the technology and development of ATMs).

[29] *See* E-mail from Ross Anderson, University of Cambridge Computer Laboratory, to Michael Froomkin (Feb. 14, 1994) (on file with author) (discussing the technology and development of ATMs).

[30] *See* SCHNEIER, *supra* note 12, at 221 (citing cryptographic standards for bank transactions). Banks rely primarily on the U.S. Data Encryption Standard (DES). *See infra* part I.B.1 (discussing how DES became the standard and why that standard is becoming increasingly vulnerable). Nevertheless, consider this disturbing boast: "'Give me $1 billion and 20 people and I'll shut America down. I'll shut down the Federal Reserve, all the ATMs; I'll desynchronize every computer in the country.'" *Technology as Weaponry*, INFO. WK., Jan. 10, 1994, at 48, 50 (quoting futurist Alvin Toffler's recollection of an unidentified intelligence official's statement).

[31] *See* DIGITAL PRIVACY AND SECURITY WORKING GROUP, ELECTRONIC FRONTIER FOUND., PRIVACY, SECURITY, AND THE NATIONAL INFORMATION INFRASTRUCTURE 2 (1993) ("Without strong cryptography, no one will have the confidence to use networks to conduct business, to engage in commercial transactions electronically, or to transmit sensitive personal information."); Hoffman et al., *supra* note 26, at 111 ("One of the consequences of an increasingly electronics-oriented economy will be the need to provide some amount of anonymity and privacy for users of such a digital cash system in order to ensure that electronic money remains anonymous and untraceable . . . ."). For a discussion of digital signatures, see *infra* Technical Appendix, part C.

techniques can be used to produce a digital signature which, when properly used, can prove that a cleartext message (such as a buy or sell order) was really sent by the party from whom the message appears to originate.[32] In addition, a digital signature attests to the integrity of the contents of a message. If the digital signature system is properly implemented, the signature of every document is uniquely calculated from the full text of the document, and is uniquely associated with the sender. There is no way to fake a signature by copying a signature from one document and attaching it to another, nor is it possible to alter the signed message in any way without the recipient immediately detecting the deception.[33] The slightest change in a signed document will cause the digital signature verification process to fail. Indeed, a signature verification failure will be caused by a transmission error affecting a single bit of the message.[34]

The proposed National Information Infrastructure, better known as Vice President Al Gore's information superhighway, envisions "telebanking" and other electronic transactions.[35] It recognizes, however, that as these services expand, so too will "public concern about communications and personal privacy."[36] One important issue will be the extent to which consumer-oriented digital payment systems allow for anonymity and privacy; another will be the extent to which law enforcement and banks will require audit trails that lead to the consumer.[37]

---

[32] *See infra* text preceding note 798 (noting that digital signatures uniquely identify the sender and connect the sender to the message).

[33] A properly generated digital signature copied from one message has an uninfinitesimal chance of successfully authenticating any other message. *See infra* note 799 and accompanying text.

[34] *See infra* text accompanying note 798.

[35] *See* Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6842, 6842 [hereinafter Inquiry on Privacy Issues] ("As the [National Information Infrastructure] develops, Americans will be able to access numerous commercial, scientific, and business data bases . . . [and] engage in retail, banking and other commercial transactions . . . all from the comfort of their homes."); *see also Microsoft and Visa to Provide Secure Transaction Technology for Electronic Commerce*, PR Newswire, Nov. 8, 1994, *available in* WESTLAW, PRNews-C database (announcing plans to provide secure electronic bankcard transactions across global public networks using RSA encryption).

[36] Inquiry on Privacy Issues, *supra* note 35; *cf.* JEFFREY ROTHFEDER, PRIVACY FOR SALE: HOW COMPUTERIZATION HAS MADE EVERYONE'S PRIVATE LIFE AN OPEN SECRET 28 (1992) ("As the population grows more computer literate and databanks become more prevalent and sophisticated, long-distance, invisible assaults on privacy will occur more frequently.").

[37] *See infra* part I.A.5 (discussing use of cryptography by criminals).

2. Businesses with Commercial and Trade Secrets

Stealing a secret is often much cheaper than discovering, or even rediscovering, it oneself. The United States annually invests more than $130 billion in nongovernmental research and development.[38] The fruits of this investment present a tempting target for industrial espionage, from both foreign and domestic competitors.[39]

Business information need not be scientific or technical to be of enormous value. Sensitive market information such as the amount that a corporation plans to bid at an auction for valuable oil leases or the amount that a construction company plans to offer at tender is of enormous benefit to a competitor.[40] Knowledge of a company's cost and price structure, market research, strategic plans, order and customer lists are of obvious benefit to competitors. For an investor, inside information such as planned merger or acquisition activity, can also reap huge profits. Encryption helps prevent high-tech eavesdropping, while at the same time discourages some low-tech theft: a stolen laptop with an encrypted disk represents a loss of hardware, but not of sensitive information.[41]

The increasing importance of intellectual property makes information security especially valuable to industry; the portability of ideas makes it ever-harder to achieve. The increase in mobile communications also plays a role. As workers rely on networks to telecommute to the office, or use cellular telephones to communicate with colleagues, or download e-mail onto their laptops while away from the office, they expose their information to eavesdroppers.[42]

---

[38] *See* ECONOMICS AND STATISTICS ADMIN. & BUREAU OF THE CENSUS, U.S. DEP'T OF COMMERCE, STATISTICAL ABSTRACT OF THE UNITED STATES 1993, at 596 [hereinafter 1993 U.S. STATISTICAL ABSTRACT]. This sum includes all research and development conducted outside the government, regardless of whether funded by industry or government.

[39] *See* GAO COMMUNICATIONS PRIVACY, *supra* note 15, at 12.

[40] *See, e.g.*, ACM REPORT, *supra* note 15, at 1 (describing electronic industrial espionage against an Alaskan oil company and by British Airways against Virgin Atlantic Airlines).

[41] *See* James Daly, *Laptop Thefts Spur Security Efforts*, COMPUTERWORLD, Oct. 12, 1992, at 1, 12 (discussing theft of laptops to obtain corporate plans, and the ways devised by firms to deny access to information on laptops).

[42] *See* Key Escrow: Its Impact and Alternatives 6 (May 3, 1994) (testimony of Dr. Whitfield Diffie, Distinguished Engineer, Sun Microsystems, Inc., before the Subcommittee on Technology and Law of the Senate Judiciary Committee) (on file with author) (discussing factors making security more essential and more difficult to achieve).

The risk to U.S. corporations of both high- and low-tech industrial espionage is particularly great because they are not just the target of domestic and foreign competitors, but also of foreign intelligence agencies. Indeed, according to the FBI, foreign governments routinely use their intelligence services to acquire valuable information about U.S. corporations.[43] As a result, without some form of communications and data security, sensitive technical and market information can be intercepted from faxes, cellular and microwave telephone calls, satellite communications, and inadequately protected computer systems.[44] Foreign firms may soon face a similar threat of industrial espionage by U.S. intelligence agencies searching for new roles, and continued appropriations, in the post-cold-war era.[45]

---

[43] According to FBI Director Louis Freeh, the governments of at least 20 nations are "actively engaged in economic espionage." Louis J. Freeh, Address at the Executives' Club of Chicago 8 (Feb. 17, 1994) (transcript available at the FBI) [hereinafter Freeh Speech]; *see also* ACM REPORT, *supra* note 15, at 1 (describing Soviet electronic surveillance of the IBM corporation in the 1970s); *id.* at 24 (describing the U.S. as the "greatest potential prey" of communications intelligence); David Silverberg, *Spy Charges Fray Ties Between U.S., France; French Officials Refute Espionage Accusations*, DEF. NEWS, May 3, 1993, *available in* LEXIS, News Library, Curnws File (describing U.S. accusations of industrial espionage by the French government allegedly aimed at 49 U.S. manufacturing companies, 26 financial institutions, and various U.S. government laboratories).

[44] *See* Freeh Speech, *supra* note 43, at 11 (urging private businesses to be vigilant in protecting valuable information such as research and development results, marketing plans, and corporate negotiating positions).

[45] CIA Director James Woolsey described economic and industrial espionage by the CIA as "the hottest current topic in intelligence." Ross Thomas, *Industrial Espionage: The CIA's New Frontier*, L.A. TIMES, July 18, 1993, at M2. The suggestion that the CIA diversify into industrial espionage received some support. *See, e.g.*, Gerard P. Burke, *Economic Espionage: Government Help Is Needed*, GOV'T EXECUTIVE, Nov. 1992, at 56 (noting that the U.S. government should attend to the "intelligence being directed against American business . . . without pause for philosophical agonizing"). It was also criticized because it was unclear how the CIA proposed to define a "foreign" corporation and how it proposed to decide which "domestic" corporations would enjoy the spoils. *See* William T. Warner, *Economic Espionage: A Bad Idea*, NAT'L L.J., Apr. 12, 1993, at 13. Later in 1993, Director Woolsey stated that for "ethical and legal reasons" the CIA had decided not to embark on the project. Tim Kennedy, *Men and Matters*, MONEYCLIPS, Dec. 12, 1993, *available in* LEXIS, News Library, Moclip File (quoting Director Woolsey's statement on Larry King Live). *But see* Robert Dreyfuss, *Company Spies: The CIA Has Opened a Global Pandora's Box by Spying on Foreign Competitors of American Companies*, MOTHER JONES, May-June 1994, at 16, 16 (suggesting that the "CIA has already begun a clandestine effort to help the American auto industry").

3. Professionals

Lawyers have long relied on ordinary telephones to communicate with clients and are increasingly using cellular telephones and electronic mail.[46] Every lawyer knows that she should never discuss client confidences in a crowded restaurant. If such a confidence is overheard by a third party, even unintentionally, waiver of the attorney-client privilege may be imputed.[47] Anyone with the right sort of receiver can overhear cellular telephone conversations. Unfortunately, the ease with which electronic mail messages can be intercepted by third parties means that communicating by public electronic mail systems, like the Internet, is becoming almost as insecure as talking in a crowded restaurant.[48] Similarly, the ease with which intruders can gain access to unprotected computers that can be accessed via the Internet means that unencrypted data on such machines is at risk.[49] Even ordinary telephone con-

---

[46] A 1993 survey by the American Bar Association Legal Technology Resource Center found that almost 75% of attorneys have a computer assigned to them. *See* Betty Cline, *Protecting Electronic Confidences*, LEGAL TIMES, June 20, 1994, at S30, S30); *see also* David P. Vandagriff, *Opening the Computer Door*, A.B.A. J., Aug. 1994, at 92, 92 (describing a law firm which relies on e-mail to communicate with and attract clients). This does not of course prove that all lawyers use their computers.

[47] Communications between a client and her attorney, made in confidence by the client when seeking legal advice, are privileged, unless this protection is waived by the client or her representative. This privilege can be waived by unintentional disclosure. *See* 81 AM. JUR. 2D *Witnesses* § 379 (1992) ("The presence of a third person indicates a lack of intention that the communications . . . are meant to be confidential."). *But see* 2 B.E. WITKIN, CALIFORNIA EVIDENCE § 1074, at 1019 (3d ed. 1986) (discussing California Evidence Code § 954, which permits the holder of the privilege to prevent disclosure of privileged communications, and extends the privilege to communications which are overheard by an "eavesdropper, finder or interceptor").

[48] *See* Jeffrey I. Schiller, *Secure Distributed Computing*, SCI. AM., Nov. 1994, at 72, 72 (suggesting an increasing frequency of "passive attacks"—eavesdropping—on the Internet). For an assessment of the security of commercial services, such as CompuServe, as a medium for attorney-client confidences, see Ronald Abramson, *Protecting Privilege in E-mail Systems*, LEGAL TIMES, Aug. 15, 1994, at 29.

Although the Internet grew out of the Defense Department network it is now insecure. As a result, the U.S. intelligence community has created the "Intelink," a secure alternative network for communications too important to be entrusted to the Internet. *See* William F. Powers, *Cloak and Dagger Internet Lets Spies Whisper in Binary Code*, WASH. POST, Dec. 28, 1994, at A4 (noting that the intelligence community created the "Intelink" because the "very public, very uncontrollable global mesh of computer networks [(the Internet)] was too risky a place to do business").

[49] *See* Peter H. Lewis, *Computer Snoopers Imperil Pentagon Files, Experts Say*, N.Y. TIMES, July 21, 1994, at A1, B10 (reporting that there "'are probably no secure systems on the Internet'" (quoting Peter G. Neumann, principal scientist at SRI International, a think tank formerly known as the Stanford Research Institute)); *see also* Terri A. Cutrera, Comment, *The Constitution in Cyberspace: The Fundamental*

versations may be at risk if the signal travels by microwave or satellite.[50] Although there are no cases to date holding that failure to encrypt a cellular telephone conversation or an electronic mail message, much less a regular phone call, constitutes professional negligence, the ease with which these can be overheard or intercepted, combined with the growing simplicity of encryption software, make it conceivable that failure to use encryption may be considered a waiver of privilege at some point in the future (at least for insecure media such as electronic mail and cellular telephones).[51]

Lawyers are not the only professionals who receive client confidences. Doctors, therapists, and accountants all receive sensitive information which they then have a duty to keep confidential. These duties can arise in tort or contract, or pursuant to state and federal statutes.[52] Some of these duties are reflected in evidentiary privileges,[53] but a privilege is not required to create the duty.[54]

4. National ID Cards and Data Authentication

Because strong cryptography can be used to authenticate data,[55] it makes nearly unforgeable national ID cards possible. The cards could have the owner's date of birth, social security number,

---

Rights of Computer Users, 60 UMKC L. REV. 139, 140-42 (1991) (surveying "hackers' skirmishes with the law").

[50] As the *ACM Report* states:

> [T]here has been a migration of communications from more secure media such as wirelines or physical shipment to microwave and satellite channels; this migration has far outstripped the application of any protective measures. Consequently, communications intelligence is so valuable that protecting its flow . . . is an important objective of U.S. national security policy.

ACM REPORT, *supra* note 15, at 24.

[51] *See, e.g.*, Cline, *supra* note 46, at S30 (describing the risks and ethical concerns of the increased use of technology in the legal field as well as the possible ways to protect confidential information).

[52] *See* Vincent M. Brannigan & Ruth E. Dayhoff, *Medical Informatics: The Revolution in Law, Technology, and Medicine*, 7 J. LEGAL MED. 1, 48-50 (1986) (noting that there are several different approaches in the law to protect patient privacy, including tort litigation and violation of state or federal privacy acts).

[53] *See, e.g.*, 81 AM. JUR. 2D *Witnesses* § 448 (1992) (describing physicians' evidentiary privileges).

[54] The recent theft of a laptop computer from the hypnotherapist who treated the Princess of Wales illustrates the dangers to doctors and their patients. After the theft, the British press began an orgy of speculation about the revelations that might emerge, *see* Edward Pilkington, *Theft from Princess's Bulimia Therapist Raises New Privacy Fears*, GUARDIAN, Aug. 1, 1994, at 3, although none did.

[55] *See generally infra* Technical Appendix, part C (discussing digital signatures).

a digitized photograph, and any other information (for example, health, immigration status, or prior convictions).[56] Users (who might include liquor stores, police, banks, employers, or a national health insurance trust) would have a reader with the government's public key on it, which they would use to decrypt the card. So long as the government was able to keep its private key secret, the ID card would be unforgeable.

National ID cards raise a host of problems outside the scope of this Article, many of which could be exacerbated by the use of cryptography. Chief among these difficulties is the danger that the government might encrypt additional information on cards that would be invisible to the holder but might be accessible to law enforcement, or even some employers. Examples of such secret information include criminal record, military discharge status, or health information.[57] Less ominously, digital signatures provide a means of authenticating all electronic data. In a world in which bank, tax, and medical records, and the contents of the digital library are all at risk of accidental or malicious alteration, authentication of data becomes critical. By providing a reliable guarantee that data with a proper signature is authentic, digital signatures provide a certain means of detecting changes when someone tries to rewrite history.

---

[56] *See* Gustavus J. Simmons, *Subliminal Communication Is ~~Possible~~ Easy Using the DSA*, *in* ADVANCES IN CRYPTOLOGY–EUROCRYPT '93: WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES 218, 219 (Tor Helleseth ed., 1994) (describing the various types of information that can and may be digitized onto an ID card).

[57] In the 1970s the Pentagon admitted that the Army was stamping discharge papers with 530 different "SPN" code numbers that gave savvy employers derogatory information about servicemen, including some with honorable discharges. The codes did not appear on discharge papers issued to servicemen but were available to employers who asked for more detailed records. Classifications included "drug abuse," "disloyal or subversive security program," "homosexual tendency," "unsuitability–apathy, defective attitudes and inability to expend effort constructively," and "unsuitability–enuresis [bed wetting]." *See* Dana A. Schmidt, *Pentagon Using Drug-Abuse Code*, N.Y. TIMES, Mar. 1, 1972, at 11. Receipt of antiwar literature sufficed to be classified as disloyal or subversive. *See* Peter Kihss, *Use of Personal-Characterization Coding on Military Discharges Is Assailed*, N.Y. TIMES, Sept. 30, 1973, at 46. In response to public pressure, the Pentagon abandoned the program and reissued discharge papers without the codes. *See Pentagon Abolishes Code on Discharges of Military Misfits*, N.Y. TIMES, Mar. 23, 1974, at 64; *Uncoded Discharge Papers Are Offered to Veterans*, N.Y. TIMES, April 28, 1974, at 33.

5. Criminals

Cryptography not only allows individuals to keep their communications and records secret, it also allows them to keep their *identities* secret. We are accustomed to more anonymity in our commercial life than we realize, although this form of privacy is shrinking. Purchasing a newspaper for a few coins from a vending machine or a store leaves no audit trail: ordinary cash is anonymous.[58] Although the use of credit cards continues to increase, there are some transactions that people prefer to keep untraceable.[59] It seems safe to suppose that some cash transactions, while legal, might not occur if the only payment option were something that leaves a record.

Cryptologists have worked out protocols for untraceable, anonymous, electronic cash ("E$") that also resist illicit duplication. These permit customers to acquire E$ from a digital bank without disclosing their identity to the bank. Using high-level cryptographic techniques, the E$ is unforgeably certified as valid, but can be spent only once.[60]

Unfortunately, although cryptography allows the creation of privacy-enhancing E$ and helps ensure that an Orwellian surveillance state remains in the realm of fiction, its advantages come at a price. The same features that might make uncrackable encryption attractive to groups seeking to change the social order by lawful but unpopular means, and that protect those working towards unpopular causes from retribution, also provide security to lawbreakers. Untraceable E$ may help make untraceable "perfect crimes" possible.[61]

---

[58] U.S. paper money is not completely anonymous, however, because each (authentic) bill carries a unique serial number and bills can be marked to facilitate tracking.

[59] For example, when my spouse and I purchase surprise gifts for each other, we tend to pay in cash because we have joint checking and credit card accounts.

[60] *See* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96, 96-97 (discussing electronic cash). *See generally infra* Technical Appendix, part C (describing digital signatures).

[61] A "perfect crime" works as follows: The criminal commits an act of extortion, for example, blackmail or kidnapping, which does not require face-to-face contact with the victim to make the demand for money. Instead of demanding small unmarked bills, the extortionist demands that the victim publish the digital signatures of a large quantity of E$ in a newspaper. Because the "payoff" occurs via publication in a newspaper, there is no danger of being captured while attempting to pick up a ransom. And because the E$ is untraceable, the extortionist is able to spend it without fear of marked bills, recorded serial numbers, or other forms of detection.

Undoubtedly, criminals and conspirators will find a use for encryption,[62] but so too will many others. Not every diarist records crimes in his daybook, but for many people there will be a certain satisfaction in knowing that their most private thoughts are safe from anyone's prying eyes, be they major governments or younger siblings.[63]

6. Users of Telephones, Electronic Mail, Faxes, or Computers

a. *Cellular Telephones*

There are at least twelve million cellular telephone subscribers in the United States.[64] Few of these telephones use encryption. Most of the cellular telephones that use some form of encryption use a very simple masking algorithm which is easy to defeat with parts available in any Radio Shack. Although cellular telephone eavesdropping is illegal,[65] it is easy.[66]

Currently, this strategy would require a sophisticated criminal, because the extortion demand would have to include the result of computations based on large random numbers, but not the random numbers themselves. These computational results would be used by the digital bank as inputs for its production of the verified E$ and would not only ensure the untraceability of the E$ but also prevent anyone but the criminal—who is the only one who knows the large random numbers—from using the E$ whose digital signatures are published in the newspaper. *See* Sebastiaan von Solms & David Naccache, *On Blind Signatures and Perfect Crimes*, 11 COMPUTERS & SECURITY 581, 582-83 (1992) (describing the mathematical steps that must be followed in order to effectuate a "perfect crime"). If, however, digital money becomes commonplace, all the necessary functions will be built into easily available software. This may not be too far away. *See* Peter H. Lewis, *Attention Shoppers: Internet Is Open*, N.Y. TIMES, Aug. 12, 1994, at D1 (describing the purchase of a compact disc via the Internet by using digital signatures and high-grade cryptography to encrypt a credit card number).

[62] *See, e.g.*, Dan Lehrer, *Clipper Chips and Cypherpunks*, 259 NATION 376, 376 (1994) (describing William Steen's use of PGP to encrypt what sheriff's deputies claimed was potential evidence of traffic in child pornography). Similarly, the defendant in *Commonwealth v. Copenhefer* would have benefitted from encryption. *See* 587 A.2d 1353, 1355-56 (Pa. 1991) (holding that an additional warrant was not required to retrieve incriminating data "deleted," but still recoverable, from the defendant's computer's hard disk).

[63] *See infra* text accompanying note 761.

[64] *See* Hoffman et al., *supra* note 26, at 111.

[65] *See* 18 U.S.C. § 2511 (1988) (providing that "any person who . . . intentionally intercepts . . . any wire, oral, or electronic communication . . . shall be fined . . . or imprisoned not more than five years, or both").

[66] *See* John Markoff, *Electronics Plan Aims to Balance Government Access with Privacy*, N.Y. TIMES, Apr. 16, 1993, at A1, A18 ("[C]ellular phone calls can be monitored by anyone with an inexpensive scanner.").

b. *Standard Telephones*

Currently, only the U.S. government has a large network of secure telephones, and they are expensive.[67] Although AT&T has developed secure telephones based on the Clipper Chip that will provide encrypted communications so long as both parties have a Clipper-equipped telephone, most telephone conversations remain vulnerable to legal and illegal wiretapping and, if the signal travels by microwave or satellite, to other forms of interception as well.[68]

c. *Faxes*

Faxes are as vulnerable to interception as any other telephone call, yet few fax transmissions are encrypted.[69] Fax interception equipment is "relatively inexpensive" and in some countries is routinely used by telephone companies or the government to monitor fax traffic.[70] Consequently, software vendors are now adding encryption options to common operating systems such as Microsoft's Windows.[71]

Encryption also protects against the consequences of misdialing a telephone number and reaching the wrong fax machine—an increasingly common problem as the number of dedicated fax lines grows.

d. *E-mail*

The exponential growth in the Internet's popularity has fueled the private demand for encryption.[72] Military-grade cryptography, or something close to it, is easily available free to any user of the Internet who knows how to download a file.[73]

---

[67] *See* ACM REPORT, *supra* note 15, at 10 (referring to "the government's STU-III secure telephone system, which is inaccessible to the general public").

[68] *See supra* note 50.

[69] *See* Hoffman et al., *supra* note 26, at 111.

[70] *New AT&T Security Device Targets Spying by Fax*, PR Newswire, June 13, 1994, *available in* LEXIS, News Library, Curnws File.

[71] *See Microsoft At Work Fax Software Debuts in Windows for Workgroups 3.11*, Business Wire, Oct. 5, 1993, *available in* LEXIS, News Library, Curnws File.

[72] *See* Hoffman et al., *supra* note 26, at 111.

[73] *See* SCHNEIER, *supra* note 12, at 437. The most popular program is Phil Zimmermann's Pretty Good™ Privacy (PGP™), currently in MIT freeware version 2.6.2 for noncommercial use only, and for commercial use in PGP Viacrypt version 2.7. *See* Philip Zimmermann, *PGP™ User's Guide Volume I: Essential Topics* (Oct. 11, 1994), *available online URL* ftp://net-dist.mit.edu/pub/PGP [hereinafter *PGP™ User's Guide*]. PGP is available to U.S. and Canadian residents for file transfer protocol

e. *Personal Records*

Many people have things they want to hide from their colleagues or family members. The secret can be as trivial as a planned surprise party, as personal as a love letter or sexual orientation, or as unsavory as a planned theft or past misdeed. It can be a private diary or the plans for a bomb. These records may be on paper or stored on a computer disk. Some people derive a sense of security from the knowledge that their communications and data are safe from unauthorized snooping by their friends, family, or anonymous computer hackers. Others seek an even greater sense of security by attempting to encrypt their communications and records in a manner that cannot be decrypted even by authorized law enforcement.[74]

7. Dissidents and Others

Most, if not all, of the readers of this Article probably experience life in the United States as one of political freedom. For some of these readers, a desire for communications and electronic records security, particularly security from possible or suspected government surveillance or intrusion, may appear to be an excess of libertarian paranoia. The existence of low-water marks in civil liberties (such as the 1798 Alien and Sedition Act,[75] the 1920s'

(FTP) from rtfm.mit.edu. Ftp is the file transfer program by which documents and program files can be retrieved from any computer on the Internet where they have been placed for public copying.

In order to comply with U.S. export restrictions, however, the Massachusetts Institute of Technology requires that would-be downloaders read the warnings located in a file whose name changes every 30 minutes before obtaining the short-lived access code needed to download the program. Foreign residents, or those with less patience, can download the file by connecting to an English server: ftp://ftp.ox.ac.uk/pub/crypto/pgp, or a German server: ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/pgp, and then selecting the appropriate sub-directory for the operating system and PGP version of their choice. For an excellent introduction to PGP, see SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY (forthcoming Jan. 1995).

[74] *See infra* part I.C.1.a (discussing law enforcement's view of the importance of electronic intelligence gathering).

[75] The Alien and Sedition Act made it a crime to publish "false, scandalous and malicious writing" against the United States government, Congress, or the President, with intent to excite "hatred" against them. 1 Stat. 596, 596 (1798). The Act, supported primarily by the Federalist Party, did not make it a crime to excite hatred against the Vice President or publish falsehoods about him because the Vice President at the time was Thomas Jefferson, who was not a Federalist. *See generally* JAMES M. SMITH, FREEDOM'S FETTERS: THE ALIEN AND SEDITION LAWS AND AMERICAN CIVIL LIBERTIES (1956) (discussing the background, enforcement, and implications of the

"Palmer raids,"[76] the Japanese internment during World War II,[77] and COINTELPRO[78]) may be seen by some readers as well-documented and anomalous departures from American ideals; other readers may see them as symptoms of a more general tendency of those in authority, approaching the "iron law of oligarchy."[79]

Organized government intrusion into personal communications and data privacy is less visible than an order to round up thousands of civilians. It is also far more frequent. When given the duty and authority to identify threats to national security,[80] public servants have shown a tendency to adopt a "vacuum cleaner[]" approach to private information.[81] Indeed, the Senate committee charged with investigating domestic surveillance noted "the tendency of intelligence activities to expand beyond their initial scope" and stated that government officials "have violated or ignored the law over long periods of time and have advocated and defended their right to break the law."[82]

Alien and Sedition laws).

[76] *See* WILLIAM PRESTON, JR., ALIENS AND DISSENTERS: FEDERAL SUPPRESSION OF RADICALS 1903-1933, at 208-37 (1963) (describing the secret, mass roundups in the 1920s of some 10,000 immigrants and others active in the labor movement, the Socialist Party, the Communist Party, and other dissident groups; their interrogation without access to counsel or bail; the illegal seizure of their records; the attempts to extort confessions from them; and the FBI investigations of government officials who sought to ensure due process for these arrestees).

[77] *See* Exec. Order No. 9066, 7 Fed. Reg. 1407 (1942) (authorizing internment camps); *see also* Korematsu v. United States, 323 U.S. 214, 217-18 (1944) (rejecting several constitutional challenges to the internment of U.S. citizens of Japanese descent pursuant to the Act); Hirabayashi v. United States, 320 U.S. 81, 100-01 (1943) (rejecting an equal protection challenge to a curfew order pursuant to the Act); Act of Mar. 21, 1942, Pub. L. No. 77-503, 56 Stat. 173 (criminalizing the refusal to comply with internment orders of a military commander). *See generally* Eugene V. Rostow, *The Japanese American Cases–A Disaster*, 54 YALE L.J. 489 (1945) (describing and criticizing the treatment of Japanese aliens and U.S. citizens of Japanese origin during World War II).

[78] *See* FRANK J. DONNER, THE AGE OF SURVEILLANCE: THE AIMS AND METHODS OF AMERICA'S POLITICAL INTELLIGENCE SYSTEM 20 (1980) (arguing that COINTELPRO, an FBI counterintelligence program, is a form of punishment directed at individuals or readily identifiable groups for past actions without trial, and is thus an attainder).

[79] ROBERT MICHELS, POLITICAL PARTIES 15 (Eden Paul & Cedar Paul trans., 1962) (arguing that "oligarchy . . . is an intrinsic part of bureaucracy or large-scale organization").

[80] National security is defined as the "national defense and foreign relations" of the United States. Exec. Order No. 12,356, 47 Fed. Reg. 14,874 (1982), *reprinted in* 50 U.S.C. § 401 (1988).

[81] S. REP. NO. 755, 94th Cong., 2d Sess., pt. 2, at 4 (1976) [hereinafter CHURCH COMMITTEE REPORT].

[82] *Id.* at 4, 5.

It is harder to view fears of government surveillance as aberrational when one learns that in the 1950s the FBI identified 26,000 "potentially dangerous" persons who should be rounded up in the event of a "national emergency," and that it maintained this list for many years.[83] During the 1970s, even sympathizers dismissed as fantastical the claims by Black Panthers and other dissident groups that they were being wiretapped and bugged by the FBI. These allegations proved to be correct.[84] Indeed, the U.S. government has an unfortunate recent history of intrusion into private matters. During the 1970s, the FBI kept information in its files covering the beliefs and activities of more than one in four hundred Americans;[85] during the 1960s, the U.S. Army created files on about 100,000 civilians.[86] Between 1953 and 1973, the CIA opened and photographed almost 250,000 first class letters within the U.S. from which it compiled a database of almost 1.5 million names.[87] Similarly, the FBI opened tens of thousands of domestic letters, while the NSA obtained millions of private telegrams sent from, to, or through the United States.[88]

Although the Constitution guarantees a high degree of political freedom and autonomy, "[t]he Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power."[89] Certainly, neither statutory nor constitutional prohibitions have proved consistently effective in preventing civil liberties abuses. For example, U.S. Census data is supposed to be private, and that privacy is guaranteed by law. Nevertheless, during World War II the government used census data to identify and locate 112,000

---

[83] *Id.* at 7, 54-57. By 1958, the FBI had whittled down the list to only 12,870 names, but the FBI placed the names it removed from the round-up list on its "Communist Index" (renamed the "Reserve Index" in 1960) for "priority consideration" for "action" after the first group had been detained. *Id.* at 55-56.

By 1972, the FBI had access to the fingerprints of more than 85 million U.S. residents. *See* Morris D. Forkosch, *Freedom of Information in the United States*, 20 DEPAUL L. REV. 1, 97 n.347 (1971).

[84] *See* SANFORD J. UNGAR, FBI 137 (1975) (describing wiretapping of the Black Panthers).

[85] *See* CHURCH COMMITTEE REPORT, *supra* note 81, at 6 (noting that the FBI had 500,000 domestic intelligence files, many with more than one name included).

[86] *See id.* at 6.

[87] *See id.*

[88] *See id.* at 6, 58-59.

[89] *Id.* at 5.

Americans of Japanese ancestry who were then transported to internment camps.[90] Similarly, the CIA repeatedly violated the prohibition on domestic intelligence contained in its charter.[91]

One need not believe that such excesses are routine to sympathize with those who fear that another such excess is foreseeable. Indeed, whether one considers these operations to have been justified, to have resulted from a type of a bureaucratic rationality that rewards results regardless of legal niceties,[92] or to have been a form of security paranoia, this history could cause a reasonable person to fear she might someday be swept up in an investigation.[93] The passage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III),[94] designed to define standards for the use of wiretaps, appears to have reduced greatly the amount of illegal wiretapping by police. Nonetheless, illegal wiretapping by police has not been completely eliminated.[95]

---

[90] *See* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 20, 23-25 (1983). Although the IRS Code, 26 U.S.C. § 6103 (1988 & Supp. V 1993), provides for the confidentiality of tax returns, one commentator has described this restriction as "quite permeable." Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383, 429 (1994).

[91] *See* CHURCH COMMITTEE REPORT, *supra* note 81, at 56-59 (discussing domestic CIA activities).

[92] For example, a former FBI officer stated, "We never gave any thought to [whether proposed actions were legal] because we were just naturally pragmatists. The one thing we were concerned about was this: will this course of action work, will it get us what we want . . . ." *Id.* at 968 (quoting testimony of former FBI Assistant Director for Domestic Intelligence William Sullivan).

[93] Imagine that a new client comes to consult you and says that she is about to form a new political action group. This group will organize demonstrations and will encourage a general strike to support an unpopular political or social opinion. The group intends to consult you frequently so as to stay within the bounds of the law, but it intends to use every politically and socially disruptive tactic that the law allows in order to gain the maximum audience for its platform. Your client also believes that at times some group members may conclude that extreme cases of injustice require peaceful civil disobedience. On the way out, your new client asks if you think the group should worry about having its telephones tapped by the police. What do you say?

[94] Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 211-25, *reprinted in* 1968 U.S.C.C.A.N. 237, 253 (current version at 18 U.S.C. §§ 2510-2521 (1988 & Supp. V 1993) (Electronic Communications Privacy Act of 1986)) [hereinafter Title III].

[95] The volumes of successful suppression orders demonstrate that the police wiretap more than the courts believe is justified; most suppression orders, however, involve cases where a court issued some process, if only on the basis of an inadequate foundation. Exposure of illegal, bad-faith, and warrantless wiretaps seems to have become rare, although clearly not completely a thing of the past. *See, e.g.*, Eric Schmitt, *Suffolk Officers Testify They Wiretapped Illegally*, N.Y. TIMES, Jan. 14, 1988, at B3 (reporting narcotics officers' testimony that they conducted illegal wiretaps with

Not all government intrusion into privacy is centrally organized, but that hardly makes it less intrusive. During the past five years the IRS has caught hundreds of its employees snooping into the tax records "of friends, neighbors, enemies, potential in-laws, stockbrokers, celebrities and former spouses."[96] Authorized users of the FBI's National Crime Information Center have used its databases to check up on friends and neighbors and to check backgrounds for political purposes.[97] It is an article of faith for many Americans that postal workers read the postcards they process—and not without reason when postal workers are heard to say that they "pass the really good ones around the office."[98]

A reasonable person may also be concerned about surveillance by nongovernmental actors. For instance, political campaigns are notorious for dirty tricks, including the bugging of opponents;[99] the yellow pages in any major city contain numerous advertisements for detective agencies and investigators;[100] and eavesdropping and bugging devices are readily available in stores.[101]

In light of this history of public and private intrusion into personal privacy and the growing interconnection of computers and communications envisioned by the National Information Infrastructure, it is impossible to dismiss the desire for personal communica-

---

the approval of their supervisor and the chief of the District Attorney's narcotics bureau).

[96] Robert D. Hershey, Jr., *I.R.S. Staff Is Cited in Snoopings*, N.Y. TIMES, July 19, 1994, at D1.

[97] *See* OFFICE OF TECHNOLOGY ASSESSMENT, CONGRESS OF THE UNITED STATES, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS, 2-3 (1994) (OTA-TCT-606) [hereinafter OTA INFORMATION SECURITY].

[98] Elaine Viets, *And the Winner Is: The Trashiest Ever*, ST. LOUIS POST-DISPATCH, May 29, 1990, at 3D; *see also* Mark Miller, *Vermont Writer Wins PEN Award*, WASH. TIMES, Apr. 21, 1993, at E4, *available in* LEXIS, News Library, Curnws File (quoting ex-postal worker E. Annie Proulx as saying, "I worked in the post office, and I know perfectly well that everyone loves to read postcards. . . . Not only do [the postal workers] read them, but if they get a particularly juicy one, they show it to their coworkers" (alteration in original)).

[99] *See* SAM J. ERVIN, JR., THE WHOLE TRUTH: THE WATERGATE CONSPIRACY 133-37 (1980) (discussing Nixon's electoral dirty tricks); Jonathan Alter & Richard Sandza, *When Tricks Turn Dirty*, NEWSWEEK, July 18, 1983, at 18, 18 (reporting that Jimmy Carter agreed not to bug television networks at the 1976 Democratic Convention only after a media advisor raised the specter of Watergate). *See generally* BRUCE L. FELKNOR, DIRTY POLITICS (1966) (discussing the history of dirty tricks in American politics).

[100] *See, e.g.*, BELL OF PA., CONSUMER YELLOW PAGES: PHILADELPHIA 276-77 (1994).

[101] *See* Tom Seibel, *The Spy Shop: Now Anyone Can Play James Bond*, CHICAGO SUN-TIMES, May 16, 1993, at 4, *available in* LEXIS, News Library, Majpap File.

tions and records security as pure paranoia. It may, in fact, be very sensible.

B. *The U.S. Data Encryption Standard (DES) Is Increasingly Vulnerable*

While the need for communications security grows, the officially sanctioned tools for providing that security are beginning to look dated and vulnerable.

1. How DES Became a Standard

In the early 1970s, the National Bureau of Standards (NBS), since renamed the National Institute of Standards and Technology (NIST), decided to define a national standard cryptographic algorithm.[102] The absence of a government standard, the NBS determined, caused people to use competing cryptographic products that were unable to communicate with each other.[103] The lack of interoperability among commercial cryptographic products deterred firms from using encryption when it would have been of value. Similarly, the absence of a standard kept the costs of products high and reduced the incentive to improve them. In selecting a standard cryptographic system, the NBS proposed to certify the strength of its algorithm, and thus reassure potential users that the system was strong enough to resist attack, something that most users would be unable to determine for themselves. The NBS determined that the algorithm it selected should be easy to use, strong, suitable for use in electronic devices, and yet sufficiently weak to be exportable without running afoul of export control regulations which control cryptography.[104]

---

[102] *See* Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage, 38 Fed. Reg. 12,763, 12,763 (1973) ("The increasing volume, value and confidentiality of these records regularly transmitted and stored by commercial and government agencies has led to heightened recognition and concern over their exposure to unauthorized access and use. . . . The need for protection is then apparent and urgent."); Encryption Algorithms for Computer Data Protection, 39 Fed. Reg. 30,961, 30,961 (1974) ("Because of the significant value or sensitivity of communicated and stored data, the need for adequate protection of this data from theft and misuse has become a national issue.").

[103] *See* Encryption Algorithm for Computer Data Protection, 40 Fed. Reg. 12,134, 12,134 (1975) ("In order to insure compatibility of secure data, it is necessary to establish a data encryption standard and develop guidelines for its implementation and use.").

[104] The algorithm the NBS ultimately selected did not meet all these criteria

In 1977, after several years of acrimonious public debate among professional cryptologists, the NBS selected an algorithm developed by IBM that the NSA had certified as "free of any statistical or mathematical weaknesses."[105] It is now known as the Data Encryption Standard (DES).[106] DES is a single-key cipher: the sender and the receiver use the same key to encrypt and decrypt the message. DES keys are fifty-six bits (about eight ASCII characters) long.[107] This means that there are seventy-two quadrillion (actually 72,057,594,037,927,936) different possible keys.[108] DES is approved for use by the government for its sensitive information, but not for classified information.[109]

The designation of DES as the U.S. standard was controversial, foreshadowing the current controversy over Clipper. An earlier version of the IBM project used a key with well over one hundred bits.[110] The key shrank to fifty-six bits by the time it became the U.S. standard. Critics charged that the shortened key was designed to be long enough to frustrate corporate eavesdroppers, but short enough to be broken by the NSA.[111] Some critics also feared there might be a "back door,"[112] an implanted weakness in a key

---

because other agencies considered it too strong to export. *See infra* part I.C.1.c.i (describing U.S. export control of encryption software under the International Traffic in Arms Regulations (ITAR)).

[105] BAMFORD, *supra* note 17, at 347; *see* U.S. Senate Select Comm. on Intelligence, *Unclassified Summary: Involvement of the NSA in the Development of the Data Encryption Standard, reprinted in* IEEE COMM., Nov. 1978, at 53, 53-55 (discussing the debate over the NSA involvement in the development of the algorithm).

[106] DES, issued as FIPS 46 in January 1977, was reviewed, slightly revised, reaffirmed for federal government use in 1983 and 1987, and reissued as FIPS 46-1 in January 1988; on September 11, 1992, NIST announced a third review of FIPS 46-1, DES, and reaffirmed it for another five years as FIPS 46-2. *See* Revision of Federal Information Processing Standard (FIPS) 46-1 Data Encryption Standard (DES), 58 Fed. Reg. 69,347, 69,347-48 (1993) [hereinafter FIPS 46-2].

DES is identical to the ANSI standard Data Encryption Algorithm (DEA) defined in ANSI X3.92-1981. *See* Eric Bach et al., *Cryptography FAQ (05/10: Product Ciphers Cryptology)* § 5 (Aug. 30, 1993), *available online URL* ftp://rftm.mit.edu/pub/usenet/news.answers/cryptography-faq/part05.

[107] *See* FIPS 46-2, *supra* note 106, at 69,348.

[108] *See* Garon & Outerbridge, *supra* note 26, at 179.

[109] *See* FIPS 46-2, *supra* note 106, at 69,348.

[110] *See* BAMFORD, *supra* note 17, at 346 (stating that the key was originally 128 bits long); SCHNEIER, *supra* note 12, at 221 (stating that the key was originally 112 bits).

[111] *See* BAMFORD, *supra* note 17, at 348 (noting that the if the IBM 128-bit key had been used, "[a]s opposed to the moderate $5000 price tag, each solution would have cost an unimaginable $200 septillion, or $200,000,000,000,000,000,000,000,000"); *infra* text accompanying note 776-80.

[112] "Back doors" are sometimes inaccurately called "trap doors," although

part of the encryption algorithm known as S-boxes, that would allow the agency to use computational shortcuts to break the code.[113]

The problem was exacerbated by the unwillingness of DES's creators to explain why they had chosen the particular, seemingly arbitrary, method of mixing up bits that they had selected. Cryptology is a field for the truly devious, and many cryptologists were concerned that there might be a mathematical vulnerability *intentionally* inserted by the cryptographers who designed the DES cipher. The search for such back doors in government-sponsored ciphers such as DES has been a popular pastime among suspicious cryptologists since the NBS proposed DES, yet no back door has been reported. Recently, however, academic cryptologists determined that DES's unusual algorithm is peculiarly resistant to a newly discovered mathematical attack called "differential cryptanalysis"—a technique which had not been discovered, at least in unclassified form, at the time DES became the U.S. standard. DES's inventors have since stated that they were aware in 1974 of DES's resistance to differential cryptanalysis, but kept quiet to protect national security.[114]

Export of DES is controlled by the State Department as if it were a weapon like a tank or fighter plane.[115] Financial institutions and the foreign offices of U.S.-controlled corporations routinely receive clearance to export DES if they show a need, but the State Department—presumably acting under the advice of the NSA—usually refuses to allow others to export it.

Although U.S. law ordinarily prevents Americans from selling DES-equipped encryption products to foreigners, DES is found around the world and freely sold by foreign corporations in many countries. It may be "the most widely used cryptosystem in the

---

technically a "trap door" function is one which is computationally easy in comparison to its inverse. For example, multiplying large prime numbers is much, much easier than factoring a very large number whose only factors are two large primes. *See* Brian Hayes, *The Magic Words Are Squeamish Ossifrage*, 82 AM. SCIENTIST 312, 312 (1994); *see also* 19 Authors, Essay, *The Law of Prime Numbers*, 68 N.Y.U. L. REV. 185, 188 n.14 (1993) (I had to cite it).

[113] *See* BAMFORD, *supra* note 17, at 347. For a full description of the "S-box" technique, complete with mind-numbing diagrams, see SCHNEIER, *supra* note 12, at 224-41, or Encryption Algorithm for Computer Data Protection, *supra* note 103, at 12,134.

[114] *See* SCHNEIER, *supra* note 12, at 240.

[115] Exports are controlled pursuant to the ITAR, 22 C.F.R. §§ 120-130 (1994). *See infra* part I.C.1.c.i.

world."[116] A full specification of DES is available in books sold in the United States,[117] the export of which is not controlled,[118] presumably on First Amendment grounds.[119]

2. DES Is Vulnerable to Attack

In a world where computing speed almost doubles every year, DES looks as if it has been a standard for a very long time. Its 56-bit keys look more vulnerable to attack than ever before. DES is thus approaching the end of its useful life, at least for high security information. NIST recertified DES in 1993 but suggested that its days as an official standard are numbered.[120]

Given that computer processors become cheaper every day, brute-force searches for DES keys are now well within the reach of relatively affordable, massively parallel machines.[121] A recent paper describes a brute-force attack on DES as "alarmingly economical," estimating that for $1 million one could build an optimized machine that would try fifty million keys per second and would crack a DES key in an average of 3.5 hours.[122] An investment of $10 million would produce a machine that would be expected to crack a DES key every twenty-one minutes.[123] DES-cracking remains beyond the means of the casual snooper, but is now within the means of many corporations and every government.

---

[116] ACM REPORT, *supra* note 15, at 5.

[117] *See, e.g.*, SCHNEIER, *supra* note 12, at 224-41.

[118] *See* Letter from William B. Robinson, Director, Office of Defense Trade Controls, U.S. Dep't of State, to Phil Karn (Mar. 2, 1994), *available online URL* ftp://ftp.eff.org/pub/EFF/policy/crypto/ITAR_export/Karn_Schneier_export_case/book_1st.response (noting that a book is "not subject to the licensing jurisdiction of the Department of State since the item is in the public domain").

[119] In contrast to DES, the government has classified the SKIPJACK encryption algorithm used by the Clipper family of chips. This should prevent the SKIPJACK algorithm from being exported. *See infra* note 187 and accompanying text (discussing the SKIPJACK algorithm).

[120] *See* FIPS 46-2, *supra* note 106, at 69,347.

[121] *See generally* Garon & Outerbridge, *supra* note 26, at 177-82 (arguing that DES is becoming increasingly vulnerable to attack as the cost of breaking it decreases exponentially).

[122] Michael J. Wiener, Efficient DES Key Search § 10 (Aug. 20, 1993) (unpublished manuscript, on file with author). The attack requires that the attacker have access to the plaintext as well as the ciphertext of a single message. Cryptologists call this a "known plaintext" approach. Such attacks are easier than one might suppose, because one does not need a long, known plaintext and it is often possible to infer something about the contents of the message one seeks to cryptanalyze.

[123] *See id.* § 4.

The security problem is compounded by the probabilistic nature of a brute-force key search. The strength of an algorithm is expressed in the amount of time it would take to be *certain* of finding the key by trying every possibility. The expected (average) amount of time per key is only half that amount. If, however, an attacker is engaged in a routine program of successively trying to break keys, and knows how often they are changed, the attacker will inevitably get lucky. This can be a serious threat in situations where one piece of luck will garner the attacker a large return.

Suppose, for example, that a bank which becomes concerned about the vulnerability of its DES keys decides to change the key used for interbank financial transactions every day. Does this give it security? If an attacker has a machine that is certain to break a key in a year, then the attacker has over a 0.01% chance of breaking the new key in an hour, and a 0.27% chance of breaking it in a day.[124] In plain English, the attacker has just better than a one in ten thousand chance of breaking each key in the first hour; she has a chance of about one in 370 of breaking each key before it is changed. The attacker thus can hope for a large electronic funds transfer to her bank account about once a year.[125]

Worse, the attacker does not need special computers so long as she has several of them. An attacker armed with only one 100Mhz Pentium computer would have a minuscule daily chance of success. If she links a group of 500 Pentium computers on a university network, however, her chance of cracking DES in a day rises to just above one in 40,000.[126] These are not bad odds for a lottery in which the payoff can be in the millions, and the cost of a ticket—idle

---

[124] *See* Garon & Outerbridge, *supra* note 26, at 181.

[125] In fact, there is more to a successful electronic funds transfer attack than breaking the code. Banking protocols contain other safeguards designed to thwart a "known plaintext" attack, making the calculations in the text more of a theoretical possibility than a likelihood. Letter from Dorothy Denning, Professor and Chair, Computer Sciences Department, Georgetown University, to Michael Froomkin 2 (Sept. 17, 1994) (on file with author).

[126] Garon and Outerbridge estimate a one in 200,000 chance for 512 linked machines running under 20 MIPS each, at which speed they are capable of 15,000 DES operations per second. *See* Garon & Outerbridge, *supra* note 26, at 187. Pentiums should be at least seven times as fast. *See* John Blackford, *The Promise of the P6*, COMPUTER SHOPPER, Aug. 1994, at 146 (noting that a 100Mhz Pentium is rated at 150 MIPS and that successor chips will be twice as fast). The estimate is probably low. Phil Karn recently reported using an optimized DES code on a 50 Mhz 486, and achieving more than 38,000 DES encryptions per second. *See* Posting from Phil Karn to Cypherpunks Mailing List (Aug. 6, 1994) (on file with author). Pentiums operating at 100 Mhz would probably run more than 2.5 times faster than this.

time on computers in a university network—may be zero to the user.

The idea of networks of computers harnessed together to crack a DES password may sound like science fiction, but something similar is already happening. A group of computer scientists and mathematicians recently used the Internet to harness computer time donated by 600 volunteers. Using a total of about 5000 MIPS-years[127] of processing time to make 100 quadrillion calculations over an eight month period, the group solved a problem equal in complexity to breaking a 129-digit RSA key.[128] RSA is a commercial public-key cryptosystem[129] and its keys are not precisely comparable to DES keys, but even so the problem was far harder than breaking DES's 56-bit key.[130]

3. How to Achieve Better Security

One solution to the aging DES problem may be to switch to "triple-DES." As the name suggests, in triple-DES a message is processed with DES three times, although the middle step is a decryption (with a different key) in order to make the final product

---

[127] A MIPS-year is the computer power of a computer capable of executing one million instructions per second operating for a year. Five thousand MIPS-years is approximately equal to the power of 33 100Mhz Pentiums running for a year. *See* Blackford, *supra* note 126, at 146.

[128] *See* Hayes, *supra* note 112, at 312; Gina Kolata, *100 Quadrillion Calculations Later, Eureka!*, N.Y. TIMES, Apr. 27, 1994, at A13. The problem, known as RSA-129, was first publicized in the Mathematical Games column of *Scientific American* in 1977. The challenge was to factor 114,381,625,757,888,867,669,235,779,976,146,612,010, 218,296,721,242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,705, 058,989,075,147,599,290,026,879,543,541. *See* Martin Gardner, *Mathematical Games: A New Kind of Cipher That Would Take Millions of Years to Break*, SCI. AM., Aug. 1977, at 120, 123. The problem remained unsolved for 17 years. The answer, 5000 MIPS-years later, was the factors 3,490,529,510,847,650,949,147,849,619,903,898,133,417, 764,638,493,387,843,990,820,577 and 32,769,132,993,266,709,549,961,988,190,834, 461,413,177,642,967,992,942,539,798,288,533. *See* Hayes, *supra* note 112, at 313. The message encoded with the 129-digit key said: "The magic words are squeamish ossifrage." *See id.* at 312.

[129] For a definition of RSA, see Paul Fahn, RSA Laboratories, *Answers to Frequently Asked Questions About Today's Cryptography* § 2.1 (Sept. 20, 1993), *available online URL* ftp://rsa.com/pub/faq/Part1; ftp://rsa.com/pub/faq/Part2; ftp://rsa.com/pub/faq/Part3 [hereinafter *RSA Cryptography Today FAQ*].

[130] Brute-force attacks on RSA keys can use shortcuts, because RSA keys are cracked by factoring large prime numbers. Shortcuts exist for this problem so that not every possible number needs to be tested. "A rule of thumb suggests that adding 10 decimal digits to the length of a number [used as an RSA key] makes it from five to 10 times as hard to factor." Hayes, *supra* note 112, at 316. Adding the same number of decimal digits to DES would result in a larger increase in the computational complexity of a brute-force keysearch.

compatible with regular DES.[131] The advantage of using triple-DES rather than a single 56-bit encryption is that messages remain more compatible with existing equipment; the disadvantages are a loss in speed, a need to revise existing software and hardware, inelegance, and some lingering uncertainty as to its safety.[132] NIST has been silent on the security (or lack thereof) of triple-DES. The NSA has not disclosed whether it considers triple-DES insecure, too secure, or neither.[133] It may be that the NSA has been silent on triple-DES in the hopes that it will be elbowed out of the market by "escrowed" encryption products such as Clipper. Triple-DES is probably very hard to break; breaking through Clipper's protections will involve no (computational) effort for authorized persons because the government will keep a copy of the keys.[134]

---

[131] *See* Wiener, *supra* note 122, § 9 (providing a schematic for triple-DES encryption).

[132] Some versions of triple-DES use a different key each time, while others reuse the first key for the final round. The two-key version is estimated to be 10^{13} times as resistant to a brute-force attack. Triple-DES is estimated to be even more secure. *See id.*

[133] The alternatives are legion. The NSA might not want to certify a cipher it knew to be insecure, although it also might not wish to let it be known that a cipher considered secure by others was in fact vulnerable. The most likely explanation, however, is that triple-DES is so secure as to be computationally infeasible to break.

The hypothesis that the NSA opposes triple-DES because it is too hard to break gains support from the NSA's lobbying campaign to discourage the X9 secretariat of the American Bankers Association from undertaking a standards development process that might lead to the adoption of triple-DES as an approved option for domestic and international financial transactions. The NSA, which is a member of the X9 group, gave several reasons for its opposition, including:

- The government is committed to EES and triple-DES is inconsistent with this objective.
- Triple-DES is not exportable.
- "[F]urther proliferation of triple-DES is counter to national security and economic concerns."

NSA Reasons for Negative Vote (Oct. 18, 1994) (circulated with X9 letter ballot) (copy on file with author). Ultimately, after a reballoting of its executive committee, the X9 membership decided to undertake the standards development process for triple-DES by forwarding the issue to its X9F Subcommittee on Data and Information Security. *See* Letter from Cindy Fuller, Associate Director X9 Secretariat, to Michael Froomkin (Jan. 31, 1995) (on file with author).

[134] Indeed, NIST has stated that no publicly available cipher was suitable as the new national standard because such a cipher could be used without escrow. *See* National Institute of Standards and Technology, Key Escrow Initiative Questions and Answers 3 (July 29, 1993) (on file with author) [hereinafter Key Escrow Initiative Q&A]. NIST selected SKIPJACK in order to "assure[] no one can use the algorithm in non-escrowed systems." *Id.* The idea is to maximize the possibility that no one will be able to use SKIPJACK with a key shielded from the government.

A second solution, applicable only to time-sensitive information, is to change DES keys very frequently. If a new DES key is used for every message, by the time the attacker figures out the old key, it is too late. Of course, this solution does not work for things that need to be kept secret for long periods of time. It also requires that parties to communication have some way to agree on a continuing supply of new keys which, by definition, they cannot do on the insecure channel which requires the encryption in the first place.[135]

A third solution is to abandon DES, in whole or in part, and try something new. The U.S. government has selected a replacement for DES that involves escrowed encryption using a new algorithm called SKIPJACK. The government has indicated that it hopes U.S. users of cryptography will adopt this option.

C. *The Escrowed Encryption Standard (EES)*

The industrialized world is in the opening stages of an "ongoing telecommunications revolution with still undefined potential to affect the way we communicate and develop our intellectual resources."[136] These changes can be liberating, and they can be painful; some have distributional consequences affecting relative power as well as access to information.

The increases in personal privacy and communications security promised by cryptography come at the expense of those who benefit from insecure communications. If every telephone call is routinely encrypted, domestic law enforcement agencies, such as the FBI and local police forces, will find wiretapping harder or even impossible. If information on computers is routinely encrypted, police may find evidence inaccessible or incomprehensible. When sophisticated encryption technologies are used abroad, intelligence agencies such as the NSA, which routinely seek to penetrate the communications of foreign powers, find their missions complicated. To the extent

---

Because the SKIPJACK algorithm at the heart of the Clipper Chip is classified, it has not had the benefit of almost 25 years of determined attack by academic cryptologists. Even though the NSA spent 10 years developing SKIPJACK, *see id.* at 2-3, this lack of publicity leaves open the possibility that it has an intentional or unintentional back door, something that seems very unlikely with DES.

[135] Chaining, in which each secure message contains the key to the next message, will work only where the same two parties send each other a continuous stream of messages and are certain that the delays between messages will be short. If there are any significant delays, the stream becomes vulnerable to probabilistic attack. *See supra* text accompanying notes 124-25.

[136] Turner Broadcasting Sys., Inc. v. FCC, 114 S. Ct. 2445, 2451 (1994).

that American citizens are better off because wiretaps help catch and convict criminals, and to the extent that communications intelligence protects the national interest from foreign threats, developments that impede legitimate wiretaps may make us all worse off.

The fear of losing electronic surveillance capabilities because of advances in encryption technology has produced a three-pronged reaction from the law enforcement and intelligence communities. First, their spokespersons have begun a public relations offensive designed to explain why these capabilities matter.[137] Second, they have sought legislation requiring that telephone networks and other similar communications channels be designed in a manner that facilitates wiretapping.[138] Third, they have designed and supported EES, best known in its most famous implementation, the Clipper Chip, which enables the government to keep a copy of the key needed to decrypt all communications using EES. These activities share the premise that it is reasonable for the government to request, and in some cases require, that private persons communicate in a manner that makes interception by the government at least practical and preferably easy.

1. Why the Government Wants EES to Replace DES

"What! fear not, man, but yield me up the keys."[139]

The Administration[140] makes two types of arguments in favor of EES. In its hard sell, the Administration, primarily through the

---

[137] *See, e.g.*, Freeh Speech, *supra* note 43.

[138] On October 25, 1994, President Clinton signed the digital telephony bill. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994). Both houses of Congress passed the bill shortly before the end of the legislative session. *See* 140 CONG. REC. S14666 (daily ed. Oct. 7, 1994) (reporting the Senate's passage of the bill by voice vote); 140 CONG. REC. H10917 (daily ed. Oct. 5, 1994) (reporting the House's passage of the bill by two-thirds vote); *see also* Sabra Chartrand, *Clinton Gets a Wiretapping Bill That Covers New Technologies*, N.Y. TIMES, Oct. 9, 1994, at A27.

On the digital telephony bill, see generally Jaleen Nelson, Comment, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139 (1994) (arguing that legislation requiring communication through only certain media and also requiring communication providers to affirmatively assist the government in wiretapping is inconsistent with rights of free flow of information and privacy in U.S. and international law).

[139] WILLIAM SHAKESPEARE, THE THIRD PART OF KING HENRY VI act 4, sc. 7, l. 37 (Andrew S. Cairncross ed., Methuen & Co. Ltd. 1964).

[140] It is clear that plans for EES have been gestating for years in the national security bureaucracy. Because, however, the Clinton Administration has adopted them wholeheartedly, this Article refers to the plan as the Administration's proposal.

FBI, paints a lurid picture of law enforcement stripped of an essential crime-detection and evidentiary tool—wiretapping—while pornographers, drug dealers, terrorists, and child molesters conspire via unbreakable ciphers, storing their records and child pornography in computers that become virtual cryptographic fortresses. Meanwhile, the intelligence agencies, primarily the NSA, quietly murmur that existing policies have proved ineffective in preventing the increasing use of unescrowed encryption, and suggest that their proposals should be adopted to prevent developments that might (or might not, they won't say) undermine the nation's communications intelligence capabilities.

In its soft sell, the government argues that if the NSA has designed a cryptographic system that it is willing to certify as secure and make available to the American public, the government has an obligation to take steps to prevent that cipher from being used against it by criminals and foreign governments. In fact, the current national standard cipher, DES, is strong enough that the U.S. government has sought to prevent its export and may indeed regret having let the algorithm become publicly available.[141] EES, the argument goes, just maintains the status quo. Even if everyone used a Clipper-equipped telephone, telephone conversations would be no less secure against legitimate government wiretapping than they are today, while being more secure against illicit eavesdropping.[142]

a. *Domestic Law Enforcement*

According to FBI Director Louis Freeh, electronic intelligence, especially wiretapping, is crucial to effective law enforcement: if the FBI and local police were to lose the ability to tap telephones because of the widespread use of strong cryptography, the "country [would] be unable to protect itself against terrorism, violent crime, foreign threats, drug trafficking, espionage, kidnapping, and other crimes."[143]

From the statistics available, it is difficult to determine how

---

[141] "With hindsight, the intelligence community might consider the public disclosure of the DES algorithm to have been a serious error and one that should not be repeated." ACM REPORT, *supra* note 15, at 25.

[142] *See* Stewart A. Baker, *Don't Worry, Be Happy: Why Clipper Is Good for You*, WIRED, June 1994, at 100, 100 (debunking seven "myths" about key escrow encryption).

[143] Freeh Speech, *supra* note 43, at 13; *see also* OTA INFORMATION SECURITY, *supra* note 97, at 9-10 (noting increasingly frequent portrayals of cryptography as a threat to domestic security and public safety).

much difference wiretaps actually make.[144] The FBI estimates that wiretaps play a role in an average of 2200 convictions per year,[145] but it is unclear how many of these convictions could have been obtained without wiretaps. Despite an almost 50% increase since 1983, court-ordered wiretaps are still relatively rare: only 919 were authorized in 1992 for all federal, state, and local police forces.[146] Of these, only 141 wiretap orders covered electronic devices such as faxes, digital display pagers, voice pagers, cellular phones, or electronic mail. In 1993, the 976 active court-ordered wiretaps allowed police to hear approximately 1.7 million conversations involving nearly 94,000 persons. The listeners described about 20% of the conversations as incriminating.[147] The law enforcement community suggests that wiretaps make the biggest difference in the largest cases because wiretaps have been used to gather evidence in 90% of the terrorism cases brought to trial.[148] The average cost of a wiretap was $57,256 in 1993,[149] so it may be that the biggest cases are the only ones in which the expense of monitoring a telephone line seems justified.[150]

Statistics aside, it seems only logical that the spread of strong, user-friendly cryptography would increase the risk that evil people will be able to frustrate law enforcement attempts to crack their computers or bug their telephones. Whether the risk has yet

---

[144] Title III authorizes the use of wiretaps. *See* 18 U.S.C. § 2516 (1988 & Supp. V 1993). Orders for pen registers, which record the telephone numbers called but not the content of the conversation, are much more frequent than wiretap orders. Also, not every wiretap order necessarily falls under Title III.

[145] *See Communications and Computer Surveillance, Privacy and Security: Hearing Before the Subcomm. on Technology, Environment and Aviation of the House Comm. on Science, Space, and Technology*, 103d Cong., 2d Sess. 10 (1994) (statement of James Kallstrom, Special Agent in Charge, Federal Bureau of Investigation) [hereinafter Kallstrom Statement] (indicating that, in the 10-year period ending in 1992, more than 22,000 convictions have resulted from court-authorized surveillances); ADMINISTRATIVE OFFICE OF THE U.S. COURTS, 1993 REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 6 (1993) [hereinafter WIRETAP REPORT] (stating that in 1993 "a total of 2,428 persons [were] arrested as a result of electronic surveillance activity; of those arrested, 413 were convicted").

[146] *See* Kallstrom Statement, *supra* note 145, at 3; WIRETAP REPORT, *supra* note 145, at 4 (showing fluctuations between 600 and 1000 court-ordered wiretaps per year between 1983 and 1993).

[147] *See* WIRETAP REPORT, *supra* note 145, at 5.

[148] *See* Hoffman et al., *supra* note 26, at 115.

[149] *See* WIRETAP REPORT, *supra* note 145, at 5.

[150] For an interesting analysis of the costs and benefits of wiretapping, which concludes that the digital telephony bill is not cost-effective, see Robin Hanson, *Can Wiretaps Remain Cost-Effective?*, COMM. ACM, Dec. 1994, at 13.

manifested itself is less clear. For all its predications of disaster in the making, "the FBI has not been able to point to a single instance to date [(September 1994)] where encryption has hampered [its] investigation of a case."[151]

Nevertheless, the fear that rogue cryptography might allow "terrorists, drug dealers, and other criminals"[152] to evade law enforcement seems to supply a large part of the motivation for the Administration's support for EES. One can only sympathize with officials who were, no doubt, asked whether they wished to go down in history as the individuals responsible for letting loose a technology that might someday hamper the investigation of a terrorist threat to a large population center.[153] Faced with the FBI's Manichaean vision of, on the one hand, a world of rampant cryptography in which the bad guys remain impregnable behind cryptological walls and, on the other hand, an ambitious plan to return to the status quo ante in which the police remain able to intercept and understand most if not all electronic communication, it is not surprising that the Clinton Administration opted for what must have appeared to be the safer course.

---

[151] Hoffman et al., *supra* note 26, at 115. Similarly, the FBI warns that the conversion of telephone networks to digital and fiber-optic systems threatens to "make it impossible for the FBI to carry out court-approved surveillance in life-and-death cases." Freeh Speech, *supra* note 43, at 12. According to FBI Director Louis Freeh, "Development of technology is moving so rapidly that several hundred court-authorized surveillances already have been prevented by new technological impediments associated with advanced communications equipment." *Id.* at 13.

The Electronic Privacy Information Center (EPIC) recently filed suit under the Freedom of Information Act (FOIA) to force the FBI to release internal studies which formed the basis for testimony to Congress that new technologies were already having a harmful effect on law enforcement's wiretapping capabilities. *See* Electronic Privacy Information Center, Press Release, *Group Seeks Release of FBI Wiretap Data, Calls Proposed Surveillance Legislation Unnecessary* (Aug. 9, 1994). The FBI is resisting the suit. *See* Telephone Interview with David Sobel, Legal Counsel, Electronic Privacy Information Center (Nov. 29, 1994).

[152] Office of the Press Secretary, The White House, *supra* note 20, at 1.

[153] Even an enthusiastic defender of an absolutist vision of the First Amendment conceded that an "absolute" right against being tortured might nonetheless find room for an exception in the case of "the man who knew where the [atom] bomb [was ticking, but] sat grinning and silent in a chair" far from the place he had planted it. Charles L. Black, Jr., *Mr. Justice Black, The Supreme Court, and the Bill of Rights*, HARPER'S, Feb. 1961, at 63, *reprinted in* THE OCCASIONS OF JUSTICE: ESSAYS MOSTLY ON LAW 89, 99 (1963). Explaining this position in a Constitutional Law class I attended at Yale in 1984, Professor Black stated that he believed torture morally justified in this extreme and hypothetical case. Once the torturer extracted the information required, Black continued, he should at once resign to await trial, pardon, and/or a decoration, as the case might be.

b. *Intelligence-Gathering*

The communications intelligence capabilities of the United States are a subject "characterized by secrecy even greater than that surrounding nuclear weapons."[154] Unclassified discussion of the effect of strong private cryptography on the capabilities of intelligence agencies quickly becomes conjecture. We do know, however, that two of the most important functions of the NSA are to acquire and decrypt foreign communications, and to conduct traffic analysis of foreign and international communications.

The two functions are related, but different. Acquisition and decryption of foreign communications are the stuff of headlines: listening to the Soviet President's telephone calls made from his limousine or breaking German codes during World War II. Traffic analysis is more subtle, but no less important. It is the study of the sources and recipients of messages, including messages that the eavesdropper cannot understand. In wartime, traffic analysis allows intelligence agencies to deduce lines of command. Changes in the volume and direction of traffic can signal the imminence of operations.[155]

Widespread foreign access to even medium-grade cryptography makes it more difficult for U.S. communications intelligence to select the messages that are worth decrypting, or even worth reading.[156] Worse, it makes traffic analysis much more difficult. So long as most electronic communications are unencrypted, intelligence agencies are able to sort messages in real time, and identify those of interest, or those which warrant further attention.[157]

---

[154] ACM REPORT, *supra* note 15, at 23.

[155] *See, e.g.*, KAHN, *supra* note 6, at 8 (discussing the U.S. Navy's use of traffic analysis to determine the movements of Japanese forces in World War II).

[156] *See* BAMFORD, *supra* note 17, at 359 (quoting then-NSA Director Bobby Ray Inman as warning: "Application of the genius of the American scholarly community to cryptographic and cryptanalytic problems, and widespread dissemination of resulting discoveries, carry the clear risk that some of the NSA's cryptanalytic successes will be duplicated, with a consequent improvement of cryptography by foreign targets.").

[157] *See* ACM REPORT, *supra* note 15, at 25.

> The goals of U.S. export control policy in the area of cryptography are (i) to limit foreign availability of cryptographic systems of strategic capability, namely, those capable of resisting concerted cryptanalytic attack; (ii) to limit foreign availability of cryptographic systems of sufficient strength to present a serious barrier to traffic selection or the development of standards that interfere with traffic selection by making the messages in broad classes of traffic (fax, for example) difficult to distinguish . . . .

Id.

Furthermore, if most traffic is plaintext, then ciphertext cries out for attention—here is someone with something to hide. Even if the message cannot be decrypted quickly, the source can be flagged for traffic analysis, which enables the intelligence agency to build up a picture of the persons with whom the source communicates. If everyone is using strong cryptography, then the most secret messages no longer stand out.

c. *Failure of Laws Designed to Prevent the Spread of Strong Cryptography*

The United States has several long-standing laws and policies designed to prevent strong cryptography from spreading abroad, and even from being widely used at home. Although these may have served to slow the spread of strong cryptography, ultimately they have failed to stop it. The following is only a brief summary of two exemplary policies and their effects.[158]

i. Export Control: The ITAR

U.S. export control is designed to prevent foreigners from acquiring cryptographic systems that are strong enough to create a serious barrier to traffic analysis, or that are difficult to crack.[159] Two sets of regulations govern the export of encryption software: the Export Administration Regulations (EAR) govern "dual use" technologies[160] and the International Traffic in Arms Regulations (ITAR) apply to items that the government considers inherently military in nature.[161] The EAR are generally less demanding, but the ITAR take precedence.[162] Under the ITAR regime, applica-

---

[158] For a general survey of high-technology export controls, see Peter Swan, *A Road Map to Understanding Export Controls: National Security in a Changing Global Environment*, 30 AM. BUS. L.J. 607 (1992).

[159] *See* ACM REPORT, *supra* note 15, at 25.

[160] 15 C.F.R. §§ 768-99 (1994). The EAR are administered by the Bureau of Export Administration in the Department of Commerce. The statutory authority for the EAR, the Export Administration Act of 1979, 50 U.S.C. app. § 2401-2420 (1988 & Supp. IV 1992), lapsed on August 20, 1994. *See* 50 U.S.C.A. app. § 2419 (West Supp. 1994). President Clinton issued an executive order requiring that the EAR be kept in force to "the extent permitted by law" under the International Emergency Powers Act (IEPA), 50 U.S.C. §§ 1701-1706 (1988 & Supp. IV 1992). *See* Exec. Order No. 12,924, 59 Fed. Reg. 43,437 (1994).

[161] *See* 22 C.F.R. § 121.1 (XIII)(b)(1) (1994). The ITAR are administered by the Office of Defense Trade Controls in the Department of State. If the State Department chooses, it can transfer jurisdiction of an export application to the Commerce Department. The statutory authority for the ITAR is the Arms Export Control Act, codified as amended at 22 U.S.C. § 2778 (1988 & Supp. IV 1992).

[162] *See* Evan R. Berlack & Cecil Hunt, *Overview of U.S. Export Controls*, *in* COPING

tions to export cryptographic software as strong as (or stronger than) DES are routinely denied.[163] Only strong products that lack

---

WITH U.S. EXPORT CONTROLS 1994, at 11, 26 (PLI Com. Law & Practice Course Handbook Series No. A-705, 1994) (arguing that "under-staffing, technically complex applications, [and] many layers of review within DOD . . . [as well] as between DOD and State" characterize the permit application process under the ITAR); Ira S. Rubinstein, *Export Controls on Encryption Software*, *in* COPING WITH U.S. EXPORT CONTROLS 1994, *supra*, at 177, 194 (stating that, under the ITAR, the State Department's Office of Defense Trade Controls (DTC) has primary jurisdiction over cryptographic software). The export of articles or services on the U.S. Munitions List is regulated by the DTC under the ITAR. *See* 22 C.F.R. § 120.5 (1994). The DTC settles disputes regarding whether an item is on the U.S. Munitions List according to the commodity jurisdiction procedure, which determines whether the ITAR or the EAR will apply. *See* 22 C.F.R. § 120.4 (1994).

Whether the ITAR unconstitutionally restrict free speech is outside the scope of this Article. For a discussion of this topic, see Constitutionality of the Proposed Revision of the International Traffic in Arms Regulations, 5 Op. Off. Legal Counsel 202, 213-14 (1981) (finding that the ITAR have constitutional and unconstitutional applications, and that they should be narrowed so that they are less likely to apply to certain protected speech); Christine Alexander, *Preserving High Technology Secrets: National Security Controls on University Research and Teaching*, 15 LAW & POL'Y INT'L BUS. 173, 203 (1983) (noting that export controls on technology raise constitutional issues because technical expression may be considered speech and because such controls infringe upon the right of academic freedom); Mary M. Cheh, *Government Control of Private Ideas–Striking a Balance Between Scientific Freedom and National Security*, 23 JURIMETRICS J. 1, 22 (1982) (arguing that cryptographic information is protected by the First Amendment); James R. Ferguson, *Scientific Inquiry and the First Amendment*, 64 CORNELL L. REV. 639, 654-56 (1979) (arguing that scientific inquiry merits some degree of protection by the First Amendment); Harold P. Green, *Constitutional Implications of Federal Restrictions on Scientific Research and Communication*, 60 UMKC L. REV. 619, 643 (1992) (suggesting that the national security basis of governmental restrictions on scientific freedom may be weak because it is impossible to hold national security secrets effectively for even short periods of time); Ruth Greenstein, *National Security Controls on Scientific Information*, 23 JURIMETRICS J. 50, 76-83 (1982) (arguing that noncommercial scientific communication should receive full First Amendment protection and noting that the ITAR may be unconstitutional unless interpreted narrowly because they may lack ties to compelling government interests); David A. Wilson, *National Security Control of Technological Information*, 25 JURIMETRICS J. 109, 128-29 (1985) (suggesting that research contracts be used as devices for implementing the ITAR to avoid the constitutional difficulties associated with requiring licenses); Roger Funk, Comment, *National Security Controls on the Dissemination of Privately Generated Scientific Information*, 30 UCLA L. REV. 405, 441-44 (1982) (arguing that current export control laws are overbroad in their restriction of speech and therefore employ excessive means to protect national security); Kenneth J. Pierce, Note, *Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation*, 17 CORNELL INT'L L.J. 197, 213-19 (1984) (arguing that the ITAR's licensing requirement is an unconstitutional prior restraint of protected speech); Allen M. Shinn, Jr., Note, *The First Amendment and the Export Laws: Free Speech on Scientific and Technical Matters*, 58 GEO. WASH. L. REV. 368, 397-400 (1990) (arguing that the regulation of scientific expression that would be unconstitutional if imposed directly would also be unconstitutional if imposed by contract).

[163] *See supra* part I.B.1 (discussing how DES became a standard in the United

the capability of being adapted for encryption, or which are designed for specific banking applications, receive official export clearance.[164]

The ITAR have failed to prevent the spread of strong cryptography. The ITAR prohibit export of cryptographic software,[165] nevertheless software created in the United States routinely and quickly finds its way abroad. For example, when version 2.6 of PGP, a popular military-grade cryptography program, was released in the United States by graduate students at MIT as freeware,[166] a researcher at the Virus Test Center at the University of Hamburg, in Germany, received a copy within days from an anonymous remailer.[167] He then placed it on his internationally-known Internet distribution site.[168] As would-be sellers of cryptographic products have frequently testified to Congress, the major effect of the ITAR is to prevent U.S. companies from competing with those foreign companies that sell sophisticated cryptographic software abroad.[169]

States).

[164] *See* OTA INFORMATION SECURITY, *supra* note 97, at 154; *see also* GAO COMMUNICATIONS PRIVACY, *supra* note 15, at 6-7, 24-28.

[165] *See* 22 C.F.R. § 121.1(XIII)(b) (1994) (designating cryptographic software as auxiliary military equipment). The ITAR state: "Software includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair." 22 C.F.R. § 121.8(f) (1994).

[166] Freeware is software which is provided for distribution at no charge by the author, although the author typically retains the intellectual property rights. *See supra* note 73 (discussing the accessibility of Phil Zimmermann's PGP).

[167] *See* E-mail from Vesselin Bontchev, Research Associate, Virus Test Center, University of Hamburg, to Michael Froomkin (July 22, 1994) (on file with author) (stating that Bontchev received a copy of PGP 2.6 from a chain of anonymous remailers and put it on the university's FTP site). According to an e-mail sent to the author by a person requesting anonymity, someone also uploaded a copy to a popular Linux archive site (sunsite.unc.edu). Overnight, therefore, the many sites around the world that mirror sunsite faithfully and unwittingly distributed PGP 2.6 worldwide.

[168] For the curious, the URL is ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/pgp/2.6mit. Other copies quickly appeared at Internet distribution sites in England, Italy, and other European countries.

[169] *See, e.g.*, *Privacy Issues in the Telecommunications Industry: Hearings on the Administration's "Clipper Chip" Key Escrow Encryption Program Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 103d Cong., 2d Sess. (May 3, 1994) [hereinafter *Clipper Chip Hearings*], *available in* WESTLAW, USTestimony Database, 1994 WL 231119, at *13-26 (testimony of Stephen T. Walker, President, Trusted Information Systems, Inc.) (summarizing studies showing how export controls harm U.S. business); *see also* Charles L. Evans, Comment, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. INT'L L. & COM. REG. 469, 481-82 (1994) (indicating that, because most countries do not have export controls

Meanwhile, enforcement of the ITAR has produced absurd results. The State Department has refused to license the export of a floppy disk containing the exact text of several cryptographic routines identical to those previously published in book form.[170] The refusal was all the more bizarre because the book itself was approved for export.[171] The only reasons given by the State Department for its refusal were that "[e]ach source code listing has been partitioned into its own file and has the capability of being compiled into an executable subroutine,"[172] and that the source code is "of such a strategic level as to warrant" continued control.[173] The State Department also concluded that the "public domain" exception to the ITAR[174] did not apply and—most bizarrely of all—that its decision was consistent with the First Amendment.[175]

ii. "Classified at Birth"

The Inventions Secrecy Act[176] gives the Commissioner of Patents the authority to issue patent secrecy orders. Even if the government has no ownership interest in the invention, the orders block the issuance of a patent and place the application under seal. If the Nuclear Regulatory Commission or the Department of Defense states that publicizing the invention would be detrimental to the national security, the patent will be withheld "for such period as the national interest requires."[177] Willful disclosure of an invention covered by a secrecy order is a criminal offense.[178] While the application of the Inventions Secrecy Act to privately

---

on encryption software, U.S. software developers are concerned about losing their foreign market shares).

[170] *See* Letter from Martha Harris, Deputy Assistant Secretary for Export Controls, U.S. Dep't of State, to Philip R. Karn, Jr. (Oct. 7, 1994) (ODTC Case CJ 081-94) (on file with author). The source code was published in *Applied Cryptography*. *See, e.g.*, SCHNEIER, *supra* note 12, at 519-32 (listing the source code for the IDEA cipher).

[171] *See* Letter from William B. Robinson to Phil Karn, *supra* note 118.

[172] Letter from William B. Robinson, Director, Office of Defense Trade Controls, U.S. Dep't of State, to Phillip R. Karn, Jr. (May 11, 1994), *available online URL* ftp://ftp.eff.org/pub/EFF/Policy/Crypto/ITAR_export/Karn_Schneier_export_case/floppy_2nd.response.

[173] Letter from Martha Harris to Philip R. Karn, Jr., *supra* note 170.

[174] *See* 22 C.F.R. § 120.10(5) (1994); *see also* Rubinstein, *supra* note 162, § 3 (describing the limited reach of the public domain exception).

[175] *See* Letter from Martha Harris to Phillip R. Karn, Jr., *supra* note 170.

[176] 35 U.S.C. §§ 181-188 (1988 & Supp. V 1993) (codified as "Secrecy of Certain Inventions and Filing Applications in Foreign Country").

[177] *Id.* § 181.

[178] *See id.* § 186.

created cryptographic devices has sometimes occasioned publicity,[179] most devices covered by secrecy orders are invented at government expense.[180]

The existence of a number of high-level cryptographic algorithms in public circulation, some patented,[181] some not, suggests that the Inventions Secrecy Act has been far from successful at preventing the spread of strong cryptography.[182]

2. How Clipper Works

> "Here, here, here be my keys; ascend my chambers;
> search, seek, find out."[183]

The Escrow Encryption Standard is designed to provide users with communications that are secure against decryption by all third parties except authorized agents of the U.S. government. Before a Clipper Chip is installed in a telephone,[184] the government will permanently inscribe it with a unique serial number and a unique encryption key. The government will keep both of these numbers on file. In order to reduce the danger that the file might be stolen or otherwise compromised, the chip's unique encryption key will be split into two pieces, each held by a different "escrow agent." The escrow agents will be required to guard the segments and release them only to persons who can demonstrate that they will be used for authorized intercepts. Reuniting the pieces of a chip's unique key gives the government the capability to decrypt any Clipper conversations.

---

[179] *See* BAMFORD, *supra* note 17, at 354-58 (describing the national publicity surrounding the NSA's issuance of secrecy orders to two inventors of cryptographic devices).

[180] *See id.* at 355-56 ("Of the three hundred or so secrecy orders issued each year, all but a very few are either on inventions the government has originated itself and already classified, or on inventions somehow connected with the government.").

[181] RSA is an example of a high-level cryptographic algorithm in circulation which has been patented. The issue of the validity of algorithmic patents is outside the scope of this Article.

[182] *Cf.* Ferguson, *supra* note 162, at 659-61 (examining how the First Amendment limits effective regulation of scientific research and publication).

[183] WILLIAM SHAKESPEARE, THE MERRY WIVES OF WINDSOR act 3, sc. 3, ll. 149-51 (H.J. Oliver ed., Methuen & Co. Ltd. 1971).

[184] The text uses the Clipper Chip, which is designed for use in telephones, as an example. Similar procedures apply to the Capstone Chip and Fortezza PCMCIA card, although those also include circuitry supporting the Digital Signature Standard and data exchange such as electronic mail.

a. *A Tale of Three Keys*

From the user's point of view, the Clipper Chip is a black box: pick up your Clipper-equipped telephone, dial another Clipper-phone, push a red button to initiate the security feature, wait a few seconds for the two chips to synchronize, read off the character string displayed on the telephone to the other party to confirm the security of the conversation,[185] and start the conversation.[186] The conversation is scrambled with a classified algorithm called SKIPJACK, which took the NSA ten years to develop, and which the government certifies as secure for the foreseeable future.[187] What

---

[185] This prevents a "man-in-the-middle" attack by which the eavesdropper, armed with two Clipper telephones, intercepts the signal, decrypts it, records it, and then reincrypts it. In the event of such an attack, the two users will have different session keys (one with each of the attacker's phones), and will thus see different character strings appear on their readouts. *See* OTA INFORMATION SECURITY, *supra* note 97, at 65 (Box 2-7).

[186] Well, that is the theory anyway. One preliminary report suggests that the AT&T 3600c, a $1300 Clipper-equipped telephone, is difficult to use:

> The hackers who bought the things had quite a hard time getting them to work at all. There were troubles getting it set up so that it would attempt to go into secure mode, and trouble getting it to do so reliably once a pair of phones that worked were found. . . .
>
> To make the unit go into secure mode, one person pushes a red button. . . . Then the modems do their thing, making modem noises for about 20 seconds (your time may vary; AT&T manual said 10 seconds.) Once connected, the sound is very weak. We in the conference had trouble hearing when the earpiece was right next to a microphone. There was also a roughly quarter second delay (presumably this is for A/D conversion + encryption) in talking. This is a longish delay, roughly equal to an overseas satellite conversation.

Posting from Adam Shostack to Cypherpunks Mailing List (Aug. 15, 1994) (on file with author) (describing a demonstration of the AT&T 3600c at the 1994 HOPE (Hackers on Planet Earth) Conference).

[187] SKIPJACK is a single-key cipher similar to DES but with an 80-bit key. In a single-key cipher the sender and the receiver use the same key to encrypt and decrypt the message. Originally, the NSA intended SKIPJACK for government communications systems. *See* Key Escrow Initiative Q&A, *supra* note 134, at 2. The current estimate is that SKIPJACK should remain secure against brute-force attacks, despite continual increases in computing power, for at least 30 years. *See* Ernest F. Brickell, et al., SKIPJACK Review Interim Report: The SKIPJACK Algorithm 1 (July 28, 1993), *available online URL* http://www.quadralay.com/www/Crypt/Clipper/skipjack-review.html [hereinafter SKIPJACK Interim Report] ("[T]here is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years.").

Not only is the SKIPJACK algorithm used by the Clipper Chip classified, but it is burned into the chip in a fashion "which is highly resistant to reverse engineering (destructive or non-destructive) to obtain or modify the cryptographic algorithm." FIPS 185, *supra* note 14, at 6004. NIST's description of its "state of the art" anti-reverse engineering design mentions three techniques: the use of nonmetallic links

happens during those few seconds before the conversation begins, and why, are the essence of EES and the source of controversy.

From the government's point of view, EES relies on three keys: the *session key*,[188] the *chip key*, and the *family key*. The session key is what SKIPJACK uses to encrypt and decrypt the conversation. Every conversation has a new session key, and any third party seeking to eavesdrop on the conversation would need to have the session key to decrypt the conversation. Oddly, the Clipper Chip does not select the session key; indeed, the Clipper Chips do not care how the telephones do this.

Suppose Alice wants to have a secure conversation with Bob. Alice calls Bob, then pushes the red button. At this point, the two Clipperphones have to agree to a session key according to a method selected by the manufacturer. The maker of the Clipperphone is free to use as secure a method as she likes. The two Clipperphones might, for example, use a supersecure method of agreeing on the session key which is so safe that two strangers who have never met before can agree on a session key in public while being overheard, and yet anyone who overhears what they say will still be unable to work out what the key is.[189] Assume that Alice and Bob use telephones that have this supersecure selection method built in. Once the two telephones agree on the session key, each phone feeds the key to its Clipper Chip.[190] As soon as the Clipper Chips are

---

to hold the "write once" information programmed on to the chip which it claims "cannot be investigated externally"; the addition of "ghost logic" which is additional random or intentional circuits with no purpose other than to confuse analysis; and "false heat dissipation methods." National Inst. of Standards and Technology, Reverse Engineering Protection, 3 FIPS 185 Docket at tab 3. NIST also noted that reverse engineering tends to destroy the device being examined, and that because every chip will have differences, these differences also provide a layer of protection. *See id.*

Nevertheless, one commentator on the proposed FIPS concluded that, based on his review of the literature and his experience in teaching a class in reverse engineering at MIT, "[p]hysics tells us that we can find out what is in these chips. Others WILL perform this analysis. The only question is when. I believe it is 3-9 months." Comments of Thomas F. Knight, Jr., 2 FIPS 185 Docket.

[188] A session key is the sequence of bits allowing decryption that will be used for only a single communication, one e-mail, or one telephone call. *See infra* text accompanying notes 790-91.

[189] One such supersecure method is the Diffie-Hellman Key Exchange. *See infra* text following note 792.

[190] Both Clipper Chips in a telephone conversation use the same session key to encrypt and decrypt their messages. The original Clipper proposal envisaged two keys, one for each chip in a telephone conversation, but NIST revised the standard to require only a single key. The NIST revision came in response to a comment it

told the session key, they begin the Clipper telephone session. The first step in a Clipper telephone session is to undermine the eavesdropper-proof creation of the session key by transmitting the session key in encrypted form for the benefit of any public servants who may be listening.

At the start of every Clipper session, a Clipper Chip sends a stream of data called a Law Enforcement Access Field (LEAF).[191] Unless Bob's Clipper Chip receives a valid LEAF from Alice's chip, Bob's chip will not talk with it.[192] As can be seen from the Figure on page 756, the LEAF is built in layers. At the center lies the session key. The chip encrypts the session key with the unique chip key. It then appends the sending chip's serial number and a checksum, then reencrypts the data with the family key, which is a master key held by the government.[193]

---

received which noted that a two-key system would limit law enforcement executing a wiretap on Alice to her side of the conversation unless it obtained a warrant for every Clipper Chip that communicated with Alice's telephone. *See* FIPS 185, *supra* note 14, at 6001. Capstone will generate its own keys. *See* MYKOTRONX, INC., CAPSTONE MYK-80: A NEW BREAKTHROUGH IN ENCRYPTION TECHNOLOGY 1 (1993) (sales literature, on file with author) (stating that the MYK-80 features "Message Encryption Key generation").

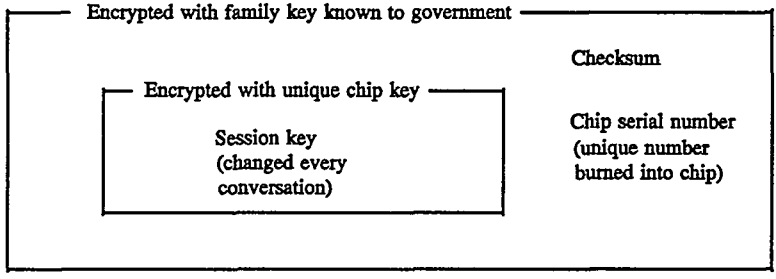
[191] The chips also send each other an "initialization vector" of unspecified length, which NIST defines as a "mode and application dependent vector of bytes used to initialize, synchronize and verify the encryption, decryption and key escrow functions." FIPS 185, *supra* note 14, at 6004.

[192] In a two-way real-time communication, the two chips send each other a LEAF, and each chip performs a check to ensure that the other LEAF is valid. In one-way communications, like e-mail, there is only one chip sending one LEAF, which will later be checked by the receiving chip. The difference is significant. If only one chip sends a LEAF, then a wiretapper will need to obtain the chip unique key for every chip which calls the line being tapped, potentially resulting in the compromise of a large number of chips. By contrast, if the LEAFs go both ways, the wiretapper is indifferent as to who started the conversation because she always has one LEAF she can decipher.

[193] The exact makeup of the LEAF is classified. *See* FIPS 185, *supra* note 14, at 6004. It is known, however, that it consists of the 80-bit session key which has been encrypted with the unit key, a 32-bit serial number unique to each Clipper Chip, and a 16-bit checksum. *See* National Inst. of Standards and Technology, Technical Fact Sheet on Blaze Report and Key Escrow Encryption 1-2 (June 2, 1994). A checksum is a "computer technique for ensuring the integrity of an identifying number." JOHN M. CARROLL, COMPUTER SECURITY 334 (1977).

FIGURE

Anatomy of a LEAF



Family key—shared by all chips, key known to government.
Chip key—unique to each chip, split between escrow agents, and indexed by chip serial number.
Checksum—a computation using the session key and other data as inputs.

In short, eavesdroppers seeking access to the session key must use two keys to decrypt the LEAF: the family key (which is common to all chips) and the chip key (which is different for every chip). Assuming that the family key will be in fairly wide circulation,[194] the security of the Clipper Chip stands or falls on the security of the master list of chip keys. This list, or the two lists of key segments, would be of enormous value to any attacker, such as a foreign government bent on industrial espionage. The way in which the keys are created, and the method by which they are held and released, are critical elements of the user's security.

When a public servant engaged in a lawful wiretap first comes across a Clipper session, she records it, including the LEAF. The public servant must now acquire the family key if she does not already possess it. According to NIST, the family keys will not be transmitted to law enforcement personnel, but will instead be stored

---

[194] Supporters of the Clipper Chip challenge this assumption. Because the family key will be in circulation only by means of a special circuit board which will be inserted into a personal computer operated by law enforcement agents, supporters of the Clipper Chip argue that its distribution will be relatively limited. *See, e.g.*, Dorothy E. Denning & Miles Smid, *Key Escrowing Today*, IEEE COMM., Sept. 1994, at 58, 58 (emphasizing that the family key is secret and only accessible to authorized government officials).

in special circuit boards capable of being installed in ordinary PCs.[195] Once decrypted with the family key, the LEAF reveals the serial number of the Clipper Chip and also reveals the encrypted session key. The public servant must then contact the two escrow agencies, giving them the chip's serial number and a legally valid reason for the wiretap, usually in the form of a warrant from a state court, a federal court, or the special Foreign Intelligence Surveillance Act (FISA) court.[196] The requestor must "certify that [the] necessary legal authorization for interception has been obtained to conduct electronic surveillance regarding these communications."[197] How this certification operates when the legal basis

---

[195] *See Clipper Chip Hearings*, *supra* note 169, *available in* Westlaw, USTestimony Database, 1994 WL 231122, at *4 (statement of Jo Ann Harris, Assistant Attorney General, Criminal Division, U.S. Department of Justice) (describing the decrypt processor). As this Article went to press, the law enforcement community had access to one of the two existing decrypt processors, although Clipper-equipped telephones are currently being shipped to government purchasers. *See* Telephone Interview with Miles Smid, Security and Technology Group Manager, National Institute of Standards and Technology (Feb. 9, 1994).

[196] *See* U.S. Dep't of Justice, Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III (Feb. 4, 1994) [hereinafter Title III Authorization Procedures] (establishing procedures by which escrow agents could release keys in response to requests pursuant to Title III), *in* Office of the Press Secretary, The White House, Key Escrow Encryption: Announcements-February 4, 1994 (Feb. 15, 1994) (information packet accompanying press release) (on file with author) [hereinafter Key Escrow Announcements]; U.S. Dep't of Justice, Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to FISA (Feb. 4, 1994) [hereinafter FISA Authorization Procedures] (same, pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1811 (1988)), *in* Key Escrow Announcements, *supra*; U.S. Dep't of Justice, Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to State Statutes (Feb. 4, 1994) [hereinafter State Authorization Procedures] (same, pursuant to state statutes or Title III), *in* Key Escrow Announcements, *supra*.

The Attorney General's procedures for release of key escrow components require that the request for key components include the agency and individual conducting the wiretap, as well as the termination date of the period for which the intercept will be authorized. *See* U.S. Dep't of Justice, Attorney General Makes Key Escrow Encryption Announcements 2 (Feb. 4, 1994) [hereinafter Attorney General's Key Escrow Announcements], *in* Key Escrow Announcements, *supra*.

U.S. foreign intelligence agencies have the authority to listen in on all forms of electronic communication, including telephones, without seeking a warrant if the communications are between foreign powers or are signals (other than spoken communication) from a foreign country, embassy, or consulate to another foreign party. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1811 (1988); *see also* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 811-13 (1989) (describing FISA procedures).

[197] State Authorization Procedures, *supra* note 196, at 1; Title III Authorization

is "exigent circumstances" (which is determined by the same officer who would be requesting the key segment), is not explained,[198] perhaps because warrantless wiretaps based on exigent circumstances are relatively rare.[199] There remains some doubt as to how the NSA and other agencies in the national security community will obtain keys. It is notable that in a recent meeting involving the FBI, the NSA, and AT&T's Bell Labs, the "the NSA did not answer a question as to whether the national security community would obtain keys from the same escrow mechanism for their (legally authorized) intelligence gathering or whether some other mechanism would exist for them to get the keys."[200]

The escrow agents have no duty to make any independent inquiries as to the adequacy of the certification before releasing the key segments.[201] Once satisfied that the wiretap request appears legitimate (in that it comes from someone authorized to make a request and contains her certification that adequate legal authority exists), the escrow agents are required to disclose the key segments for the key for which the serial number was submitted. The public servant requesting the key fragments puts them together and uses

---

Procedures, *supra* note 196, at 1; FISA Authorization Procedures, *supra* note 196, at 1.

[198] The Attorney General's procedures require that requests for key segments be made by the principal prosecuting attorney of a state or political subdivision, or by the responsible person in an agency. *See* State Authorization Procedures, *supra* note 196, at 2. This requirement overlaps with the authority for emergency wiretaps in Title III, 18 U.S.C. § 2518(7) (1988).

[199] *See* CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING § 30 (1978) ("Law enforcement officials have been reluctant to use [the emergency eavesdropping] authorization for fear it is unconstitutional."); 1 WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 4.2(g) (1984) ("There has been virtually no use of this emergency power . . . ."). *But see* CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING §§ 30-30f (Supp. 1993) [hereinafter FISHMAN SUPPLEMENT] (describing various procedures for emergency wiretaps which have been used in life-threatening situations).

[200] Posting from Matt Blaze to Cypherpunks Mailing List (Feb. 2, 1994) (on file with author) (reporting surprising frankness on the part of NSA spokespersons at a meeting discussing key escrow).

[201] The Department of Justice, however, is required to ascertain, after the fact, that the legal authorization existed for Title III wiretaps and FISA wiretaps. *See* Title III Authorization Procedures, *supra* note 196, at 2 (stating that the "Department of Justice shall" ascertain the existence of authorizations for electronic surveillance); FISA Authorization Procedures, *supra* note 196, at 2 (same). Strangely, the Justice Department has no such obligation when the key segment is requested by a state or local police force. *See* State Authorization Procedures, *supra* note 196, at 2 (stating that the "Department of Justice may" inquire into the authorization for electronic surveillance).

the reconstituted chip key to decrypt the session key. Armed with the decrypted session key, the public servant can at last decrypt the conversation. Because the presence of the Clipper Chip has no effect on the applicable constitutional and statutory rules, the public servant remains obligated to minimize the intrusion.[202]

In summary, a public servant might decrypt an EES message as follows:

Public servant

(1) intercepts the message, including the LEAF (128-bit LEAF encrypted with the family key);

(2) decrypts the LEAF with the family key (32-bit chip ID, 80-bit session key encrypted with chip key, 16-bit checksum);

(3) contacts her escrow agents, reports the chip ID, and avers existence of the legal authority for the wiretap;

(4) receives two 80-bit key segments;

(5) XORs[203] the key segments to produce an 80-bit chip key;

(6) decrypts the encrypted session key with the chip key;

(7) decrypts the entire message with her decrypted session key.

b. *The Escrow Agents' Critical Role*

The Department of Commerce's NIST and the Treasury Department's Automated Systems Division will be the two escrow agents who will create and hold the key segments.[204] Both escrow agencies will participate in the creation of each Clipper Chip's unique chip key. After raw Clipper Chips emerge from the factory

---

[202] *See* 18 U.S.C. §§ 2510-2521 (1988 & Supp. V 1993).

[203] XOR is a binary operation by which two binary numbers are compared a bit at a time. If both bits have the same value then XOR returns zero; if the two bits differ, XOR returns one. Both segments are thus equally necessary to retrieve the key, and neither segment alone provides the holder with any more information about the value of the key than would be possessed by a person who held no segments at all.

An example, using a hypothetical 1-bit key divided into two 1-bit segments, *A* and *B*, may make this clearer. Even if you know that segment *A* is 1, you still have no more information about the key's value than does anyone else. If segment *B* is 0, the key is 1 (because 1 XOR 0 = 1); but if segment *B* is 1, then the key is 0 (because 1 XOR 1 = 0). Similarly, someone holding segment *B* but not *A* is equally uninformed as to the key's actual value.

[204] *See* Attorney General's Key Escrow Announcements, *supra* note 196, at 1.

they will be taken to a secure, compartmented information facility,[205] which is the vault-like room that the government uses when handling classified documents. Each of the escrow agents will provide a list of random numbers which, when combined, will provide the numbers from which the keys will be generated.[206]

After the keys are generated, the escrow agents will be given a disk containing lists of chip serial numbers and an associated 80-bit number which represents half the information needed to recreate a chip's key. Both key segments must be combined to retrieve the chip key, and neither segment alone provides the holder with any information as to the chip key's contents.[207]

Although the escrow agents do not check the bona fides of any requests for key fragments, they do require a substantial amount of paperwork before releasing a key. The escrow agents are also required to keep detailed records of key segment requests and releases. The existence of this paper trail should provide a significant disincentive to rogue wiretapping requests by agents in the field. Similarly, NIST has announced an elaborate system of safeguards to protect each Clipper Chip's unique key. The scheme

---

[205] Currently a company called Mykotronx is the only supplier authorized to produce Clipper Chips. The secure, compartmented information facility is located at Mykotronx. *See* Key Escrow Initiative Q&A, *supra* note 134, at 6. This may impose barriers to entry for potential competitors.

[206] NIST has devised a fairly elaborate procedure for the key generation process. Someone working for each of the escrow agents will type 80 characters into a computer, which will store the characters, the amount of time between the keystrokes, the date, and the time. The computer will then feed these values into NIST's secure hash algorithm to produce a number. For a discussion of the secure hash algorithm, see Approval of Federal Information Processing Standards Publication 180, Secure Hash Standard (SHS), 58 Fed. Reg. 27,712 (1993); Proposed Revision of Federal Information Processing Standard (FIPS) 180, Secure Hash Standard, 59 Fed. Reg. 35,317 (1994) (correcting a technical flaw and confirming the algorithm's security reliability). *See also* Dorothy E. Denning, *The Clipper Encryption System*, AM. SCIENTIST, July-Aug. 1993, at 319, 321-22 (describing how two escrow agents and a computer are needed to create the unit key, thus increasing public confidence that the failure of one escrow agent cannot compromise the system); Denning & Smid, *supra* note 194, at 60-61 (describing how escrow agents generate a key number and a random seed number for use in each programming session). Currently, the system is able to program about 120 Clipper Chips per hour, although NIST contemplates switching to a higher volume system at some future date. *See id.* at 64.

The procedure for generating the random numbers is important because anyone who knows which pseudorandom number generator was used and who also knows the "seed" could use this information to recreate all the keys without going to the trouble of consulting the escrow agents.

[207] Technically, the two 80-bit segments held by the escrow agents are XORed to produce the actual key. *See* Denning & Smid, *supra* note 194, at 64-65.

involves complex rationing of information and mutual monitoring by the escrow agents from the moment the Clipper Chip is created. Further security attends the inscription of the key upon a Clipper Chip, its subsequent division into two key segments, and ultimate safeguarding by the two escrow agents.[208]

The security precautions introduced by NIST in late 1994 are complex. To the nonspecialist they appear sufficient to prevent security breaches at the time the keys are "burned in" and to prevent surreptitious copying or theft of the key list from the escrow agents. But no amount of technical ingenuity will suffice to protect the key fragments from a change in the legal rules governing the escrow agents. Thus, even if the technical procedures are sound, the President could direct the Attorney General to change her rules regarding the escrow procedures. Because these rules were issued without notice or comment, affect no private rights, and (like all procedural rules) can therefore be amended or rescinded at any time without public notice, there is no legal obstacle to a secret amendment or supplement to the existing rules permitting or requiring that the keys be released to whomever, or according to whatever, the President directs. Because the President's order would be lawful, none of the security precautions outlined by NIST would protect the users of the EES system from disclosure of the key segments by the escrow agents. Nothing in the EES proposal explicitly states that the NSA will not keep a set of keys; indeed, the only way to acquire a set of EES-compliant chips is to have the device that incorporates them tested and approved by the NSA. Similarly, although the specifications for the decrypt processor call for it to delete keys when a warrant expires and to automatically send a confirmation message to the key escrow agents, the interim model (there is only one) in use by law enforcement organizations relies on manual deletion.[209]

---

[208] The procedures were devised in collaboration with the Department of Justice, the FBI, NIST, the NSA, the Department of the Treasury Automated Systems Division, and Rapid System Solutions, Inc. *See id.* at 58.

[209] *See* OTA INFORMATION SECURITY, *supra* note 97, at 65 n.5 (Box 2-7) (citing presentation by NIST Security Technology Manager Miles Smid in June 1994).

c. *Limited Recourse for Improper Key Disclosure*

The escrow system lacks legal guarantees for the people whose keys are generated by the government and held by the escrow agents. Indeed, the Attorney General's escrow procedures state that they "do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance."[210] In short, the government disclaims in advance any reliance interest that a user of an EES-equipped device might have in the government's promise to keep the key secret.[211] A victim of an illegal wiretap would have a cause of action under Title III against the wiretapper,[212] but, it appears, no remedy against the escrow agents, even if the escrow agents acted negligently or failed to follow their own procedures.[213] The Attorney General's proce-

---

[210] Title III Authorization Procedures, *supra* note 196, at 3; FISA Authorization Procedures, *supra* note 196, at 3; State Authorization Procedures, *supra* note 196, at 3. The government is completely correct to warn users of EES that their rights to exclude illegally seized or tainted evidence in any criminal proceeding are unchanged by EES.

[211] Traffic analysis using pen registers (which record the numbers called by a telephone) and trap and trace devices (which record numbers calling the telephone) do not implicate the Fourth Amendment. *See* Smith v. Maryland, 442 U.S. 735, 741-46 (1979). Under Title III, however, both pen registers and trap and traces require a court order, although an actual warrant is not required. *See* 18 U.S.C §§ 3121-3123 (1988); Criminal Procedure Project, *Twenty-Second Annual Review of Criminal Procedure: United States Supreme Court and Court of Appeals 1991-1992*, 81 GEO. L.J. 853, 952-54 (1993). Because decrypting the LEAF with the family key involves listening to at least a few seconds of the conversation, the act of intercepting and decrypting the LEAF constitutes wiretapping. This is so even though the information thus gathered is no better than could be obtained by a trap and trace device or a pen register. Perversely, however, even though the decryption of the LEAF is a wiretap, it may not violate the Fourth Amendment if the telephone user has no reasonable expectation of privacy for the LEAF. Whether a chip user would have for her LEAF a reasonable expectation of privacy, as the term is used in Fourth Amendment cases, is not as clear as it should be. The difficulty arises because the user is aware that the government has the information needed to decrypt the LEAF. Although the government has promised to use that information only in specific circumstances, the government cannot be estopped and is therefore free to renege. *See, e.g.*, Office of Personnel Management v. Richmond, 496 U.S. 414, 434 (1990) (holding that payments from the Federal Treasury may only be made if authorized by statute, and that erroneous advice given to a claimant by a government employee does not therefore estop the government's denial of the claim); Heckler v. Community Health Servs., Inc., 467 U.S. 51, 63 (1984) (noting "the general rule that those who deal with the Government are expected to know the law and may not rely on the conduct of Government Agents contrary to law"); Federal Crop Ins. Corp. v. Merill, 332 U.S. 380, 385 (1947) (holding that claimants' lack of knowledge of regulations published in the *Federal Register* does not prevent those claimants from being bound by such regulations).

[212] *See* 18 U.S.C. § 2520 (1988).

[213] If the agent knowingly released a key improperly, the agent might be a co-

dures themselves are merely directives. They are not even legislative rules, which might be subject to notice and comment restrictions before being rescinded. A future administration could, if it wanted, secretly[214] instruct the escrow agents to deliver copies of the keys to an intelligence or law enforcement agency, or even White House "plumbers," thereby violating no law or regulation (the plumbers, though, would violate Title III when they used the information).[215] Because the chip-unique keys were voluntarily disclosed to the government, the chip's owner might lack a "legitimate" (that is, enforceable) expectation of privacy in the information.[216]

If the intercepted communication were an e-mail or a file transfer, rather than a telephone call, the chip owner subject to an illegal or inadvertent disclosure by the escrow agents may be in a particularly weak position if the information ever makes its way to court: many Title III protections granted to voice communications do not apply to transfers of digitized data.[217]

Shortly before the 103d Congress adjourned, Congressman George Brown introduced the Encryption Standards and Procedures Act of 1994,[218] which would have waived the sovereign immunity of the United States for "willful" but unauthorized disclosures of key fragments by its officials—and excluded liability in all other circumstances.[219] In the absence of similar legislation, however, there

---

conspirator or abettor of the illegal wiretapper.

[214] If the executive order were not classified, it would presumably have to be disclosed pursuant to the Adminstrative Procedures Act. *See* Adminstrative Procedures Act, 5 U.S.C. § 552(a)(2)(C) (1988) (requiring agencies to make publicly available instructions to staff that affect members of the public).

[215] *See* 18 U.S.C. § 1030(a)(3) (1988) (codifying the Computer Fraud and Abuse Act, which makes it illegal to trespass into federal computer systems). Section 1030(a)(4) proscribes the use of federal computers to defraud. Section 1030(a)(5) makes illegal any unauthorized access to a computer system used in interstate commerce, as well as the alteration or destruction of records. This last provision applies only to those acting without authority. *See* § 1030(a)(5). Thus, the "plumber" would violate the statute, but arguably the escrow agent would not.

[216] *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[217] *See infra* note 329 and accompanying text (discussing the Electronic Communications Privacy Act of 1986).

[218] H.R. 5199, 103d Cong., 2d Sess. (1994).

[219] *Id.* § 31(h)(2). The Encryption Standards and Procedures Act of 1994, if enacted, would have provided:

> The United States shall not be liable for any loss incurred by any individual or other person resulting from any compromise or security breach of any

may currently be no monetary remedy even for a "willful" disclosure.

II. THE ESCROWED ENCRYPTION PROPOSAL—LEGAL, POLICY AND TECHNICAL PROBLEMS

The Clinton Administration introduced EES through a procedural back door that relies on market power to prevent a substantial increase in the communications privacy of Americans, an outcome not authorized by any statute. EES used a standard-setting procedure but failed to set an intelligible standard. The procedure violates the spirit, although not the letter, of the Administrative Procedures Act (APA).

The Administration is spending large sums of money on a controversial project in the absence of congressional authorization. This policy cuts out the legislature, and indeed the public, from the decision to proceed with EES.[220] Only Congress can intervene, because, as things currently stand, no one has standing to sue. The Administration's use of a standard-setting procedure to make substantive policy sets an alarming precedent of rule making with highly attenuated accountability.

A. *EES: The Un-Rule Rule*

1. FIPS 185: A Strange Standard

An appreciation of both the novelty and the danger of the Administration's regulatory approach requires some understanding of the regulatory device that NIST used to introduce EES. The Constitution gives Congress the power to "fix the Standard of Weights and Measures."[221] NIST (formerly the Bureau of Standards) is the agency charged with this responsibility. Federal

---

encryption standard established under subsection (b) or any violation of this section or any regulation or procedure established by or under this section by—

(1) any person who is not an official or employee of the United States; or

(2) any person who is an official or employee of the United States, unless such compromise, breach, or violation is willful.

Id.

[220] Some have argued that the process also violates the Computer Security Act of 1987. *See infra* part II.A.3.

[221] U.S. CONST. art. I, § 8, cl. 5.

Information Processing Standards (FIPS) are standards and guidelines intended to improve the federal government's use and management of computers and information technology, and to standardize procurement of those goods.[222] FIPS are also used to announce national norms in areas of changing technology where NIST believes industry would benefit from the existence of a standard. Officially, the only bodies required to conform to FIPS are agencies within the federal government (and in some cases government contractors), although in practice they are often adopted as de facto national standards by industry and the public.[223] The private sector finds FIPS attractive because they allow

---

[222] NIST issues FIPS pursuant to § 111(d) of the Federal Property and Administrative Services Act of 1949, ch. 288, 63 Stat. 379 (the Brooks Act), as amended by the Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724. Relevant parts of the authority are codified at 40 U.S.C. § 759(d) (1988 & Supp. V 1993) and 15 U.S.C. § 278g-3 (1988). Arguably, neither of these statutes gives either NIST or the Secretary of Commerce the authority over telecommunications required to issue FIPS 185, because neither statute mentions telecommunications equipment. *See* National Bureau of Standards Act of 1901, 15 U.S.C. §§ 271-278h (1988) (describing NIST's powers prior to Computer Security Act of 1987); Computer Security Act of 1987, 15 U.S.C. § 278g-3 (1988) (giving NIST power to develop "standards, guidelines, and associated methods and techniques for computer systems" and to make standards for the "cost-effective security and privacy of sensitive information in Federal computer systems," and defining the latter to include "automatic data processing equipment" (ADPE)); Federal Property and Administrative Services Act of 1949, 40 U.S.C. § 759(d)(1) (1988) (giving the Secretary of Commerce authority to "promulgate standards and guidelines pertaining to Federal computer systems"); Federal Property and Administrative Services Act of 1949, 40 U.S.C. § 759(a)(2) (1988) (defining ADPE to include "any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception, of data or information").

NIST, however, obtained a delegation of authority from the General Services Administration (GSA) to issue a FIPS relating to telecommunications system, although the GSA itself argued that the delegation was unnecessary. *See* Letter from Francis A. McDonough, Assistant Commissioner, Federal Information Resources Management, General Services Administration, to Michael R. Rubin, Deputy Chief Counsel, NIST (Jan. 28, 1994) (included in volume 3 of the official record of FIPS 185); *see also* 41 C.F.R. § 201-20.303(b)(2)(i)(B) (1993) (stating, per GSA regulation, that NIST has substantial telecommunications authority, which is arguably based on an incorrect reading of the Paperwork Reduction Reauthorization Act of 1986, Pub. L. No. 99-591, § 101(m), 100 Stat. 3341-335).

[223] *See* Department of Commerce, Semiannual Agenda of Regulations, 59 Fed. Reg. 20,135, 20,136 (1994) [hereinafter Agenda of Regulations] (noting that FIPS "apply only to the Federal Government" and that in FIPS' development, NIST "works closely with private industry standard-setting organizations"); Mitch Ratcliffe, *Security Chips Trigger Alarm: Clipper and Capstone Open Digital Back Door*, MACWEEK, Apr. 26, 1993, at 1, 1 (stating that FIPS often become de facto standards because the U.S. government is the largest computer customer in the world).

conformity with, and sales to, the government, and because the standards themselves often have technical merit, or at least reflect a technical consensus of the many public and private interests that NIST routinely consults before it promulgates a FIPS.[224] EES is FIPS 185.[225]

One of the more serious complaints about FIPS 185 is that it fails to set a standard. One member of the NIST Computer Privacy and Security Advisory Board went so far as to submit a comment calling the FIPS "content-free."[226] Most FIPS describe a conforming device or procedure in sufficient detail for the reader to understand what it is; FIPS 185 does not. Instead, it states, "Implementations which are tested and validated by NIST will be considered as complying with this standard."[227] FIPS 185 requires the use of the SKIPJACK encryption algorithm and a LEAF creation method.[228] But the standard does not define those terms because the specifications for both are classified. Instead, FIPS 185 unhelpfully notes:

> Organizations holding an appropriate security clearance and entering into a Memorandum of Agreement with the National Security Agency regarding implementation of the standard will be provided access to the classified specifications. Inquiries may be made regarding the Technical Reports and this program to Director, National Security Agency, Fort George G. Meade . . . .[229]

For an economic analysis of the costs and benefits of standards, see Stanley M. Besen & Joseph Farrell, *Choosing How to Compete: Strategies and Tactics in Standardization*, J. ECON. PERSPECTIVES, Spring 1994, at 117, 117-18 (asserting that firms manipulate standards for competitive advantage); Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, J. ECON. PERSPECTIVES, Spring 1994, at 93, 93-95 (warning that pervasive standards lead to inefficient market outcomes in "systems markets" characterized by products that require other conforming products to function). *But see* S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, J. ECON. PERSPECTIVES, Spring 1994, at 133, 133-35 (arguing that the negative effects of standards identified by Katz and Shapiro are infrequent, if they exist at all).

[224] *See, e.g.*, *USACM Position on the Escrow Encryption Standard*, COMM. ACM, Sept. 1994, at 16, 16 (reporting a press release by the Association for Computing Machinery stating that "[i]ncreasingly, the standards set through the FIPS process directly affect non-federal organizations and the public at large").

[225] *See* FIPS 185, *supra* note 14, at 6002.

[226] *Id.* at 5999.

[227] *Id.* at 6003.

[228] *See id.*

[229] *Id.* at 6005. Apparently, individuals who are not members of organizations, or organizations that do not already supply products or services to the government, need

Nor does the standard explain what sorts of devices it covers. It merely states that "[v]arious devices implementing this standard are anticipated. The implementation may vary with the application. The specific electric, physical and logical interface will vary with the implementation."[230] Admittedly, FIPS 185 at least has the good grace to acknowledge that it is "not an interoperability standard. It does not provide sufficient information to design and implement a security device or equipment. Other specifications and standards will be required to assure interoperability of EES devices in various applications."[231]

In sum, FIPS 185 says something to this effect: "Various electronic devices will contain classified components that will provide escrowed encryption using a classified algorithm. If you ask nicely, we may let you use one in your design, and we will tell you whether we approve of your device and whether we will let you produce it." This is a strange sort of standard.

2. An End-Run Around Accountability

Such an unorthodox standard is the result of an even more unorthodox procedure. FIPS 185 is not just a standardless standard; it is an un-rule rule which seeks to coerce the public by wielding federal market power to generate a de facto standard without providing any real administrative accountability. Despite conforming to the notice and comment procedure of § 553 of the APA,[232] and being duly published in the *Federal Register*,[233] FIPS 185 is not a legislative rule because it does not seek, at least on its face, to bind the public.[234] Nor, despite being on its face an

---

not apply.

[230] *Id.*

[231] *Id.* at 6001.

[232] 5 U.S.C. § 553(b)-(d) (1988). There is no reason other than long-standing practice by the NBS and NIST to believe that a notice and comment procedure was actually required. *But see* American College of Neuropsychopharmacology v. Weinberger, [1975 Developments] Food Drug Cosm. L. Rep. (CCH) § 38,025 (D.D.C. July 31, 1975) (holding that publication in the *Federal Register* combined with the complexity of the rules themselves meant that the rules in question were subject to the notice and comment procedures of § 553 of the APA).

[233] Publication in the *Federal Register* is only required if the President should disapprove or modify a FIPS. *See* 40 U.S.C. § 759(d)(1) (1988).

[234] A legislative rule is an exercise of power delegated by Congress to an administrative agency. It can create, modify or remove legal duties, rights or exemptions. Agencies may make legislative rules through formal or informal rule making. Formal rule making is rarely used. Informal rule making ordinarily requires publication of

announcement, is FIPS 185 a nonlegislative rule as the term is usually understood.[235] Familiar types of nonlegislative rules include interpretative rules, statements of policy and "publication rulemaking." FIPS 185 fits into none of these categories.[236] Interpretative rules set forth an agency's understanding of a statutory provision, a judicial or administrative decision, or another rule,[237] and FIPS 185 clearly does not provide any of these. Nor is FIPS 185 an example of what Peter Strauss has called "publication rulemaking"[238] in which agency staff, acting pursuant to APA

---

a notice of the proposed rule in the *Federal Register*, a request for comments, and then a reasoned attention to those comments before the final rule is promulgated in the *Federal Register*. *See* 5 U.S.C. § 553(b)-(d) (1988) (detailing the rule-making procedures for administrative agencies).

Most FIPS which affect federal procurement are mandatory in the sense that only federal agencies, but not the public, are required to adhere to them. *See* Agenda of Regulations, *supra* note 223, at 20,136; *see also* FIPS 46-2, *supra* note 106, at 69,347 (reaffirming FIPS 46-1 "for Federal Government use"); *cf.* Delegation of Authority for Waivers for Federal Information Processing Standards (FIPS), and of Procedures for Waivers for FIPS, 54 Fed. Reg. 4322 (1989) [hereinafter Waivers for FIPS] (establishing waiver procedures for agencies seeking exemptions from FIPS's requirements). FIPS 185 states, however, that it is "totally voluntary," even for federal agencies. FIPS 185, *supra* note 14, at 5998.

[235] A nonlegislative rule is a rule which does not exercise a power delegated by Congress to an administrative agency. It cannot create, modify, or remove legal duties, rights, or exemptions. *See* Michael Asimow, *Nonlegislative Rulemaking and Regulatory Reform*, 1985 DUKE L.J. 381, 383 (defining nonlegislative rules as those which "do not exercise delegated lawmaking power," but only "provide guidance to the public and to agency staff and decisionmakers"); Charles H. Koch, Jr., *Public Procedures for the Promulgation of Interpretative Rules and General Statements of Policy*, 64 GEO. L.J. 1047, 1048 (1976) (using the term "nonlegislative rules" to refer to rules not promulgated under the direction of the legislature and not in compliance with the APA's notice and comment procedures). If FIPS 185 is a rule at all, it is formally a nonlegislative rule in the sense that it does not attempt to create any legal obligations that bind the public.

FIPS 185 is barely a rule within the APA's definition because the only way in which it constitutes "the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy," 5 U.S.C. § 551(4) (1988), is that it allows other agencies to substitute EES products for DES products. *See* FIPS 185, *supra* note 14, at 5999 (suggesting, but not mandating, that federal managers use EES instead of DES).

[236] FIPS 185 is far too formal to fall into the miscellaneous category of agency products. This category includes press releases, informational publications, letters, etc. Such informal documents are not published in the *Federal Register*, which contains only documents "having general applicability and legal effect." Industrial Safety Equip. Ass'n, Inc. v. EPA, 837 F.2d 1115, 1121 (D.C. Cir. 1988); *cf.* Brock v. Cathedral Bluffs Shale Oil Co., 796 F.2d 533, 539 (D.C. Cir. 1986) (noting that the *Federal Register*, unlike the *Code of Federal Regulations*, also contains "policy statements" that have no legal affect).

[237] *See* Asimow, *supra* note 235, at 383.

[238] PETER L. STRAUSS, AN INTRODUCTION TO ADMINISTRATIVE JUSTICE IN THE

§ 552(a)(1)-(2), publish technical guidelines, staff manuals, or standards (such as IRS Revenue Rulings) that inform the public of the agency's likely position in future enforcement, application-and-approval, or benefit/reimbursement cases.[239] Nor is FIPS 185 a statement of policy.[240] Nothing within the four corners of FIPS 185 establishes or explicates a policy, unless giving federal agencies the option to purchase certain devices constitutes a policy.[241]

On its face, FIPS 185 is a minor internal housekeeping regulation. Whether anyone, inside or outside of the government, chooses to comply with it is entirely up to her, although FIPS 185 states that use of EES by nonfederal government organizations "is encouraged."[242] In form, EES is a description of something, as well as a grant of permission for agencies to use that something instead of other things they are currently using. Yet despite explicitly disclaiming any intention of legally binding the public, FIPS 185 is part of a strategy to coerce the public by use of the government's market power to create a de facto national standard. At the same time that the Department of Commerce promulgated EES, the Department of Justice announced that it was buying 9000 Clipper-equipped telephones, using money from its Asset Forfeiture Super Surplus Fund,[243] a fund comprised of profits from RICO,

---

UNITED STATES 157 (1989); *see also* Peter L. Strauss, *The Rulemaking Continuum*, 41 DUKE L.J. 1463, 1467 (1992) (noting that "publication rulemaking" is typically effected by agency staff without participation by the agency's head).

[239] *Cf.* Robert A. Anthony, *Interpretive Rules, Policy Statements, Guidances, Manuals, and the Like–Should Federal Agencies Use Them to Bind the Public?*, 41 DUKE L.J. 1311, 1333-40 (1992) (discussing nonlegislative documents on which agencies rely for these categories of cases).

[240] For the APA exception for policy statements, see 5 U.S.C. § 553(b)(3)(A), (d)(2) (1988).

[241] Prior to FIPS 185, agencies that did not procure waivers were required to use DES for sensitive nonclassified information. *See* FIPS 46-2, *supra* note 106, at 69,348. "Sensitive information" is defined as:

> [A]ny information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5 [United States Code] (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

15 U.S.C. § 278g-3(d)(4) (1988).

[242] FIPS 185, *supra* note 14, at 6003.

[243] *See* Office of the Press Secretary, The White House, Fact Sheet: Public Encryption Management 2 (Apr. 16, 1993), *in* "Key Escrow" Information Packet, *supra* note 20.

drug, and other asset forfeitures.[244] Expenditures from the Asset Forfeiture Super Surplus Fund require no congressional appropriations. The effect is to cut Congress out of the decision-making process on an issue which may eventually affect the privacy rights of most Americans. One need not be an opponent of EES to believe that a decision with significant potential effects on communication privacy should have been left to the legislature.

The Department of Defense, too, is considering buying millions of EES-compliant devices,[245] although this purchase may require congressional approval. The government's market power as a bulk purchaser suggests that, all other things being equal, producer economies of scale will allow EES-compliant devices to be the lowest-cost hardware-based civilian cryptography products available. In addition, EES products will have the significant advantage of being able to communicate with the government's telephones, something that any competing technology will lack.[246]

The Clinton Administration also announced that it will exempt EES products from the export ban in the ITAR.[247] If the ITAR

---

[244] *See* 28 U.S.C. § 524(c)(4) (1988 & Supp. V 1993) (listing the financial sources of this fund). The Attorney General has discretion to use this fund for law enforcement purposes and is not required to return money in the fund to the Treasury. Legitimate uses of the fund include paying informants, equipping government vehicles for law enforcement functions, and purchasing evidence. *See* § 524(c)(1). The fund is substantial, with about $1 billion in the pipeline at any time, including money due to be paid to state law enforcement agencies. *See* William P. Barr, *Attorney General's Remarks, Benjamin N. Cardozo School of Law, Nov. 15, 1992, in* 15 CARDOZO L. REV. 31, 33 (1993). The expected income alone from the Assets Forfeiture Fund in 1987 was estimated at $150 million. *See* David J. Fried, *Rationalizing Criminal Forfeiture*, 79 J. CRIM. L. & CRIMINOLOGY 328, 365 n.167 (1988) (citing *Budget Appropriations: Hearings Before the Subcomm. of the House Comm. on Appropriations*, 99th Cong., 2d Sess. 114 (1986)).

[245] The Pentagon plans to purchase about two million Capstone PCMCIA cards for the Defense Message System. *See* Messmer, *supra* note 16, at 20; *see also* OTA INFORMATION SECURITY, *supra* note 97, at 127 n.29 (citing Clinton Brooks, Special Assistant to the Director, NSA, May 25, 1994, for the statement that the Pentagon is using Tessera (now renamed Fortezza) cards in the Defense Message System).

[246] *See* Dorothy E. Denning, *The Clipper Chip Will Block Crime*, NEWSDAY (N.Y.), Feb. 22, 1994, at 35 (noting that "[t]he Justice Department has ordered $8 million worth of Clipper scramblers in the hope that they will become so widespread and convenient that everyone will use them").

[247] Travelers desiring communications security while abroad should take note that exemption from export control does not equal exemption from the paperwork attendant to even a temporary export license. Temporary export licenses for exportable secure telephones or other telephone security devices require a shipper's export declaration (SED) which must be acquired before the trip and presented (in duplicate) to Customs officers upon export and re-import. Unfortunately, Customs officials who handle passengers have no familiarity with this form, do not know where

are revised in this manner, EES products will become the only U.S.-made exportable products offering strong encryption, disadvantaging U.S-based competitors further.[248] These efforts have already had an effect: the day that the Administration announced its plans for Clipper, AT&T announced that its new secure telephone, the 3600, would not use a DES device as originally announced, but would use Clipper instead.[249]

The current Administration makes no secret of its hope that the combination of federal standard-setting, federal purchasing power, and fine-tuning of export control will allow it to impose a de facto standard on the public, even though there is no statutory authority for the standard, and even though Congress has never appropriated a penny to support the standard. In so doing, NIST has pioneered a new type of un-rule. It is a rule that the Administration indeed hopes and intends to have a "practical binding effect,"[250] but not because the rule announces to the public how the agency will act in the future, nor because the agency intends to act in compliance with the rule, nor because the rule describes safe harbors for compliance

---

it can be obtained, and are not necessarily willing to sign the SED because this function is allocated to the cargo department. At best, attempts to follow the regulations impose a minimum of an hour's delay in each direction, and probably more. *See* E-mail from Matt Blaze, Senior Research Scientist, AT&T Bell Laboratories, to Michael Froomkin (Jan. 6, 1995) (on file with author) (relating an unsuccessful attempt to go through regular channels and concluding "it just isn't possible for an individual traveler to follow all the rules").

[248] *See* Office of the Press Secretary, The White House, Statement of the Press Secretary 2 (Feb. 4, 1994) (explaining that the Department of State "will streamline export licensing procedures for [these] encryption products), *in* Key Escrow Announcements, *supra* note 196; U.S. Dep't of State, Statement of Dr. Martha Harris, Deputy Assistant Secretary of State for Political-Military Affairs: Encryption—Export Control Reform (Feb. 4, 1994) (detailing reforms of the licensing process), *in* Key Escrow Announcements, *supra* note 196.

[249] *See* Dorothy E. Denning, Encryption and Law Enforcement § 5 (Feb. 21, 1994) (unpublished manuscript, on file with author). Although government procurement regulations are designed to award contracts to the lowest conforming bidder, without regard to past services rendered on other matters, cynics may find this action to be evidence of AT&T's desire to remain in the government's good graces. Paranoids may point to then-NSA Director Lincoln D. Faurer's statement in 1981 that "our intention is to significantly reward those DOD suppliers who produce the computer security products that we need." BAMFORD, *supra* note 17, at 362. Or, it may be that AT&T believed this was the patriotic, or commercially sensible, thing to do.

[250] Anthony, *supra* note 239, at 1328; *see* Robert A. Anthony, *"Well, You Want the Permit, Don't You?" Agency Efforts to Make Nonlegislative Documents Bind the Public*, 44 ADMIN. L. REV. 31, 37 (1992); *cf.* Asimow, *supra* note 235, at 382 (suggesting that postadoption public participation is the best way to deal with practically binding nonlegislative rules).

with existing rules.[251] Rather, by issuing the rule (if a rule it be), the agency hopes to set in motion a train of events that will coerce the public's compliance.

NIST's use of a FIPS in this manner is an interesting reversal of the usual circumstance of a nonlegislative rule that an agency intends to be binding.[252] In the ordinary situation, an agency has chosen not to use the notice and comment procedure that characterizes informal rule making under APA § 553, and has simply issued the rule, perhaps labeling it "interpretative" or "policy guidance." A party seeking to challenge the rule attempts to demonstrate that the rule is actually legislative and thus invalid without notice and comment. The aggrieved party argues that it was entitled to be consulted on the rule and that the agency may not deprive the party of its right to make comments. Once the comments are duly docketed, the agency has a duty to take them seriously and may not reject them without giving nonarbitrary reasons.[253] In the classic case, the agency responds by denying the substantive import of its rule and arguing that, because the rule breaks no new ground, notice and comment are not necessary.

With FIPS 185, NIST has turned this process on its head. A proposed version of FIPS 185 was published in the *Federal Register*, and NIST solicited comments.[254] It received hundreds.[255] NIST accepted a few, but rejected many others on the disingenuous grounds that because the standard was entirely voluntary, it could cause no harm.[256] NIST thus invoked the formally voluntary

---

[251] *But cf.* Anthony, *supra* note 239, at 1328-29 (suggesting that most nonlegislative documents with a "practical binding effect" achieve this end via one of the three means described in the text).

[252] These are sometimes called "non-rule rules." Anthony, *supra* note 250, at 32 n.2 (defining "non-rule rules" as those that meet the APA's definition of "rules" but are not promulgated through legislative rule-making procedures).

[253] *See* Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 33, 34 (1983) (emphasizing the duty of administrative agencies to consider all important aspects of a problem and to "articulate a satisfactory explanation for its action").

[254] *See* A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES), 58 Fed. Reg. 40,791 (1993).

[255] *See* FIPS 185, *supra* note 14, at 5998 (stating that comments were received from "22 government organizations in the United States, 22 industry organizations and 276 individuals").

[256] *See id.* NIST ignored comments from five industry organizations and 200 individuals who stated that guarantees were needed to assure that EES would not be a first step towards prohibition of other forms of encryption. NIST responded that the standard was voluntary. *See id.* Eight industry organizations and 181 individuals said that it was premature to adopt EES as a standard until policy decisions on

nature of the FIPS as justification for dismissing the concerns of commentators who saw FIPS 185 for what it was, and what NIST itself surely understood it to be: an attempt to coerce the public through market means. NIST simply failed to address the merits of many important complaints, including those challenging the security, necessity, or wisdom of its proposal, with the result of significantly devaluing the opportunity to comment.[257] Yet, unlike most agencies that fail to address the merits of comments received on a proposed rule, NIST likely has little to fear from judicial review of its decision because there appears to be no one with standing to challenge its actions.

Even a competing product manufacturer would be unlikely to have standing to protest a procurement order for products conforming to FIPS 185.[258] As a plaintiff, such a competitor might be able to argue that had it not been for the permission to purchase the items granted in FIPS 185, the procuring agency might have purchased the plaintiff's devices instead. Such a claim would, however, be risky at best. The plaintiff would have to mount a convincing case regarding causation, somehow demonstrating that but for FIPS 185, the plaintiff's products would have conformed with the agency's requirements;[259] the plaintiff would also need to

---

encryption had been made. NIST responded that the standard was voluntary. *See id.* at 5999. Seven individuals proposed alternate technologies that they believed would be more cost effective than EES. NIST responded that the standard was voluntary. *See id.* at 6000.

[257] Section 553's notice and comment requirements reflect Congress's "judgment that . . . informed administrative decisionmaking require[s] that agency decisions be made only after affording interested persons" an opportunity to communicate their views to the agency. Chrysler Corp. v. Brown, 441 U.S. 281, 316 (1979). By requiring "openness, explanation, and participatory democracy" in the rule-making process, notice and comment assures the legitimacy of administrative norms. Weyerhaeuser Co. v. Costle, 590 F.2d 1011, 1027 (D.C. Cir. 1978).

[258] By bringing the case as a protest to a specific contract award, ideally one in which the competitor had made a tender of goods which conformed to the preexisting standard, the competitor might be able to distinguish Control Data Corp. v. Baldridge, 655 F.2d 283 (D.C. Cir.), *cert. denied*, 454 U.S. 881 (1981). In *Baldridge*, the D.C. Circuit held, effectively, that no one has standing to sue to overturn a FIPS outside of the bid protest context because the public is outside the "zone of interests to be protected or regulated by" the Brooks Act. *Id.* at 290. Bid protests of this sort go initially to the Board of Contract Appeals of the General Services Administration. *See* 40 U.S.C. § 759(f) (1988 & Supp. V 1993); *see also* Contract Disputes Act of 1978, 41 U.S.C. §§ 601-613 (1988 & Supp. V 1993).

[259] To have standing, a plaintiff must demonstrate "injury that fairly can be traced to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court." Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26, 41-42 (1976); *see also* Valley Forge Christian College

show that the agency would have been unable to obtain a waiver from the preexisting requirement that it use a DES product to protect sensitive information.[260] Without an extraordinarily good factual basis, this barrier is probably insurmountable, leaving the would-be plaintiff without the direct personal stake in the case necessary for standing.

One other possible strategy for the plaintiff would be to claim "reputational" injury to its product or firm on the grounds that the FIPS would cause customers other than the government to reject its nonconforming products. Those employing this strategy could then try to invoke *Meese v. Keene*[261] to overturn the no-standing-to-challenge-a-FIPS rule of *Control Data Corp. v. Baldridge*.[262]

Otherwise, it is very difficult to imagine who might have standing to sue to overturn FIPS 185. A party seeking relief would have to argue that the FIPS was not as harmless as NIST claimed, and that the replies to comments were therefore defective. Just as NIST was able to ignore critical comments on its draft FIPS by saying that the standard was optional and hence harmless,[263] so too could it argue that because the standard is nonbinding, no one has a legal right to demand that a court review it.[264]

Should the Administration's attempt to combine technical standard-setting authority with market power succeed, however,

---

v. Americans United for Separation of Church and State, Inc., 454 U.S. 464, 473 (1982) (applying the "injury in fact" element of the standing requirement).

[260] *Cf.* 40 U.S.C. § 759(d) (1988) (creating waiver power); Waivers for FIPS, *supra* note 234, at 4322 (permitting delegation of waiver power).

[261] 481 U.S. 465, 475 (1987) (holding that plaintiff office-holder's allegation that his constituents would be "influenced against him" by government action labeling films he sponsored as "political propaganda" sufficed to create standing).

[262] 655 F.2d 283, 295-97 (D.C. Cir.) (applying the zone of interest test to hold that plaintiff lacked standing to challenge a FIPS), *cert. denied*, 454 U.S. 881 (1981).

[263] *See supra* notes 254-57 and accompanying text.

[264] *See, e.g.*, International Tel. & Tel. Corp. v. Local 134, 419 U.S. 428, 442-48 (1975) (determining that an agency process without binding effect, even if it leads to significant practical consequences, is not reviewable under APA § 551); Industrial Safety Equip. Ass'n v. EPA, 837 F.2d 1115, 1121 (D.C. Cir. 1988) (holding that the joint publication and dissemination of a "Guide" by the National Institute for Occupational Safety and Health and the EPA, branding petitioner's wholly EPA-compliant protective device much less safe than a competitor's device, was not a reviewable action, nor a legislative rule: the Guide "established no rule that the regulated industry must obey"); American Trucking Ass'n, Inc. v. United States, 755 F.2d 1292, 1296-98 (7th Cir. 1985) (concluding that a report was an "educational undertaking" and did not "impose an obligation, determine a right or liability or fix a legal relationship," and was therefore not reviewable agency action, despite allegations of revenue loss to parties resulting from the report).

many parties will be justly aggrieved. Makers of competing products will lose market share, and perhaps may be driven out of their market altogether. Individuals who might have preferred non-escrowed encryption, if it could be obtained at or near the same price as an EES device, may find that option closed to them. Such a policy will establish a new and undesirable process by which the government will likely be able to avoid the APA in a small, but significant, class of cases.[265] Current law does not recognize any of these injuries, save perhaps the claim of lost market share, as legally cognizable.[266] A major decision as to the degree of privacy to be afforded to U.S. citizens will have been made without effective congressional or popular participation.

Placing all FIPS, or all standard-setting relating to high technology, under the APA would be one way of ensuring that the executive branch can never again use standard-setting to manipulate the market for high technology items, at least not without judicial review for reasonableness. Although this change would vaccinate against the disease, it would also have undesirable side-effects. Neither nonbinding national technical standards nor the government's internal procurement standards should be litigated.[267] If a manufacturer is dissatisfied because a national or procurement standard more closely conforms to a competitor's product than its own, the proper place to fight that battle is the marketplace, not a court. EES is a special case because the technology at issue has social implications far beyond the ordinary FIPS, and because the government is seeking to use its purchasing power to coerce the market to achieve an end other than reliability, ease of use, or technical excellence. It would be a pity if prevention of such special cases were to force so disruptive a change on a system which ordinarily seems to work reasonably well.[268]

---

[265] *See supra notes* 232-41 and accompanying text (questioning, in the context of the APA, the government's seeming nonaccountability regarding FIPS).

[266] *Cf.* Valley Forge Christian College v. Americans United for Separation of Church and State, Inc., 454 U.S. 464, 485-86 (1982) (holding that "psychological" injury is insufficient to confer standing).

[267] This is not to suggest that abuses of the standard-setting process are not properly actionable. *See, e.g.*, Allied Tube & Conduit Corp. v. Indian Head, Inc., 486 U.S. 492, 503-07 (1988) (denying *Noerr* antitrust immunity to parties who manipulated the standard-setting process of a private association without official authority).

[268] "[S]tandards are essential to the achievement of full competition and to the saving of large sums of money by the Government." Control Data Corp. v. Baldridge, 655 F.2d 283, 286 (D.C. Cir.), *cert. denied*, 454 U.S. 881 (1981). On the benefits of standardization, see Michael A. Epstein, *Standards and Intellectual Property, in*

Trying to find an avenue for judicial review of a coercive but formally voluntary FIPS is probably more trouble than it is worth.[269] The greatest procedural problem with FIPS 185 is not the absence of judicial review but the attempt to evade congressional participation in a decision that may have major social consequences for many years. The solution to this problem is logically, if not politically, simple. If the executive branch did not have funds available with which to purchase thousands of EES-equipped devices, it would have to go to Congress for the money. Congress could then debate the issue and, regardless of what it decided, the process would conform with the values of openness, explanation, and representative democracy which the un-rule rule undermines. To prevent further abuses of the FIPS procedure, either the Justice Department's Asset Forfeiture Fund should be returned to the Treasury, or its terms should be narrowed to make it clear that its proceeds cannot be used to attempt to influence product markets.[270]

3. Did NIST's Cooperation with the NSA over FIPS 185 Violate the Computer Security Act of 1987?

NIST's relationship with the NSA is poorly documented.[271] Clipper's critics argue that NIST's adoption of EES in FIPS 185 violated either the letter or the spirit of the Computer Security Act

---

INTELLECTUAL PROPERTY/ANTITRUST 1993 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. G4-3903, 1993), *available in* WESTLAW, TP-All Database.

[269] Vermont Yankee Nuclear Power Corp. v. Natural Resources Defense Council, Inc., 435 U.S. 519, 549 (1978), presents a particularly great hurdle by its holding that courts cannot impose on an agency procedural requirements not found in the APA.

[270] Narrowing the terms of the Asset Forfeiture Super Surplus Fund is very much a second-best solution. Not only would suitable amendments to the authorizing legislation be difficult to draft, but the terms of the fund are already narrow enough to force money to be spent in inappropriate ways. *See generally* Alison R. Solomon, Comment, *Drugs and Money: How Successful Is the Seizure and Forfeiture Program at Raising Revenue and Distributing Proceeds?*, 42 EMORY L.J. 1149, 1166-91 (1993) (examining the benefits, drawbacks, and management of federal asset forfeiture programs as law enforcement and revenue-raising tools).

[271] NIST takes the position that all the interesting information is classified or confidential. Computer Professionals for Social Responsibility (CPSR) filed a FOIA request to obtain documents relating to the NSA's role in FIPS 185. CPSR's challenge to the denial of their request was dismissed with prejudice on summary judgment in Computer Professionals for Social Responsibility v. National Inst. of Standards & Technology, No. 92-0972-RCL (D.D.C. Apr. 11, 1994). CPSR is currently appealing the district court's summary judgment ruling. *See* Computer Professionals for Social Responsibility v. National Inst. of Standards & Technology, No. 94-5153 (D.C. Cir. filed June 27, 1994).

of 1987[272] (Act), because, even though the Act was designed to ensure civilian control of computer security issues, NIST effectively and illegally ceded its powers to the NSA.[273] NIST and the NSA have refused to make public any information regarding their discussions that would show whether NIST complied with the Act. Consequently, it is currently impossible to make an informed judgment as to NIST's compliance with the Act.[274] All that can be said pending litigation is that NIST has not proved that it complied with the Act.[275]

The claim that NIST violated the Act draws much of its force from the legislative history of the Act and from NIST's subsequent close relationship with the NSA, which arguably violates the spirit of the Act.[276] In 1984 President Ronald Reagan issued National Security Decision Directive (NSDD) 145, which put in motion a train of events leading to the Act. NSDD 145 granted the NSA sweeping powers to make policy and develop standards for the "safeguarding" of both classified and unclassified information in civilian agencies and in the private sector.[277] This transfer to the NSA of authority

---

[272] Pub. L. No. 100-235, 101 Stat. 1724 (codified as amended at 15 U.S.C. §§ 271, 272, 278g-3 to g-4, 278h (1988 & Supp. V 1993) and 40 U.S.C. § 759 (1988 & Supp. V 1993)).

[273] *See Telecommunications Network Security: Hearings Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy and Commerce*, 103d Cong., 1st Sess. 133-35 (1993) (prepared testimony of Marc Rotenberg, Director of Washington Office, Computer Professionals for Social Responsibility); *see also* Plaintiff's Memorandum in Opposition to Defendant's Motion for Summary Judgment and in Support of Plaintiff's Cross-Motion for Partial Summary Judgment at 3-7, Computer Professionals for Social Responsibility v. National Inst. of Standards and Technology (D.D.C. filed May 18, 1993) (No. 92-0972-RCL) [hereinafter CPSR Motion] (suggesting that, contrary to the intent of Congress, NIST may have retained "surface" control of the development of DSS, but allowed the NSA to develop the technical guidelines).

[274] Nor is it clear, if the Act were violated, who would have standing to complain. *See supra* text accompanying notes 258-64.

[275] *See supra* note 271 (discussing CPSR's lawsuit against NIST).

[276] One slight complication is that NIST's authority to promulgate FIPS 185, insofar as it relates to the Clipper Chip itself (as opposed to Capstone), probably does not derive from the Computer Security Act. The Act relates to computer systems and related equipment, not telephones. NIST's authority to promulgate a telecommunications standard that applies beyond modems derives from a delegation of authority from the GSA. *See supra* note 222. The discussion in the text undoubtedly applies to more directly computer-related devices such as the Capstone Chip and the Fortezza PCMCIA card.

[277] H.R. REP. NO. 153(I), 100th Cong., 1st Sess., pt. 2, at 6 (1987), *reprinted in* 1987 U.S.C.C.A.N. 3120, 3158. For a summary of NSDD 145, see Renae A. Franks, Note, *The National Security Agency and Its Interference with Private Sector Computer Security*, 72 IOWA L. REV. 1015, 1020-24 (1987).

over civilian and especially private information was the precise evil that the Act was designed to cure.[278] The legislative history states that Congress believed that the NSA's "natural tendency to restrict and even deny access to information" disqualified it from that role,[279] and Congress therefore rejected the NSA's suggestion, made in testimony to a House committee, that the Act should formally place the NSA in charge of all government computer security.[280]

Nevertheless, the Act does not require a watertight separation between NIST and the NSA. Instead, the Act directs NIST to "draw[] on the technical advice and assistance" of the NSA "where appropriate."[281] NIST is also directed to "coordinate closely" with several other agencies, including the NSA, to avoid duplication of effort[282] and to use the NSA's computer security guidelines to the extent that NIST, not the NSA, determines they should apply.[283]

Soon after the Act became law, NIST and the NSA signed a Memorandum of Understanding (MOU) setting out a detailed regime of cooperation regarding computer and telecommunications security issues.[284] With one exception, the MOU appears to be designed to create interagency consultation and to prevent duplication of effort, as required by the Act. That exception, though, is not trivial: NIST agrees to submit "all matters" regarding "techniques to be developed for use in protecting sensitive information" in its purview to review by a Technical Working Group comprised of equal numbers of the NSA and NIST staff in order "to ensure they are consistent with the national security of the United States."[285] If the two agencies are unable to agree, then either agency can refer the matter to both the Secretary of Commerce *and*

---

[278] *See* H.R. REP. NO. 153(I), *supra* note 277, at 22, 25-26, *reprinted in* 1987 U.S.C.C.A.N. at 3137, 3141 (noting that "[g]reater emphasis should be given to cooperation between the military and civil agencies as well as the private sector in setting computer security and training goals," and stating that, although the NBS (now NIST) should work closely with other agencies such as the NSA, the NBS/NIST should retain "final authority" over the development of guidelines).

[279] *Id.* at 21.

[280] *See id.* at 7.

[281] Computer Security Act § 2(b)(1).

[282] Computer Security Act § 3(b)(6)(A), 15 U.S.C. § 278g-3(b)(6)(A) (1988).

[283] *See* Computer Security Act § 3(c)(2), 15 U.S.C. § 278g-3(c)(2) (1988).

[284] Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Pub. L. No. 100-235 (Mar. 23, 1989), *reprinted in* SCHNEIER, *supra* note 12, at 442-44 [hereinafter the NSA-NIST MOU].

[285] *Id.* at 444.

the Secretary of Defense, from where it may go to either the National Security Council or the President for an ultimate decision. Meanwhile, "[n]o action shall be taken on such an issue until it is resolved."[286]

It is clear that NIST and the NSA have had extensive contacts regarding EES.[287] Whether these contacts, and in particular the actions of the Technical Working Group, amount to a violation of the Act depends on whether EES was referred to the Technical Working Group, and on how the NIST-NSA relationship worked. The Act clearly requires NIST to make its own decisions;[288] there is no statutory authority for NIST to let the NSA make decisions for it. Just as clearly, the Act requires NIST to consult with the NSA, although it directs NIST to decide when consultation is appropriate.[289]

There is no reason, with or without the Act or the MOU, that NIST could not allow itself to be persuaded by the NSA, so long as NIST were to keep the ultimate power of decision.[290] The MOU

---

[286] *Id.*

[287] For example, according to a document dated March 26, 1990, obtained by CPSR under FOIA, at one Technical Working Group meeting the NSA provided NIST with a position paper, classified "TOP SECRET CODEWORD," that discussed "reasons for the selection of certain algorithms." CPSR Motion, *supra* note 273, at 7.

[288] *See* Computer Security Act § 2(b)(1) (stating that the "specific purposes" of the Act include assigning to NIST, and no other agency, "responsibility" for standards and guidelines for the security and privacy of federal computer systems that have nonclassified information).

[289] *See id.*

[290] Agencies are allowed to choose to defer to other opinions, so long as they make the final decision. *See* Delta Data Sys. Corp. v. Webster, 744 F.2d 197, 201-02 (D.C. Cir. 1984) (stating that an agency may accept recommendations from the GAO); City of Alexandria v. United States, 737 F.2d 1022, 1025-27 (Fed. Cir. 1984) (stating that the separation of powers doctrine requires administrative agencies to be open to persuasion by congressional committees); Westinghouse Elec. Corp. v. United States Nuclear Regulatory Comm'n, 598 F.2d 759, 775-76 (3d Cir. 1979) (holding that an independent agency may allow itself to be persuaded by the President or Congress); M. Steinthal & Co. v. Seamans, 455 F.2d 1289, 1304-05 (D.C. Cir. 1971) (noting that the GAO's significant experience in procurement contracts makes it a persuasive source of information in procurement cases); A.G. Schoonmaker Co. v. Resor, 445 F.2d 726, 728 (D.C. Cir. 1971) (upholding the Army's adoption of the Comptroller General's opinion to set aside the awarding of a bid); John Reiner & Co. v. United States, 325 F.2d 438, 442-43 (Ct. Cl. 1963) (holding it was not arbitrary or capricious for an executive agency to defer to the GAO, an arm of the legislature, in order to promote interbranch comity, even if at first the agency disagreed with GAO's views), *cert. denied*, 377 U.S. 931 (1964); Henry Spen & Co. v. Laird, 354 F. Supp. 586, 588 (D.D.C. 1973) (allowing a procurement officer to be convinced by the Comptroller General, even when the latter lacks jurisdiction); United States *ex rel.* Brookfield Constr. Co. v. Stewart, 234 F. Supp. 94, 100 (D.D.C.) (holding that a disbursement

between the NSA and NIST does, however, suggest two scenarios that would violate the Act. If the working group deadlocked on some issue, or took votes in which the two NIST members were outvoted four-to-two (or three-to-two), and if NIST changed its policies as a result of either of these votes,[291] then NIST would no longer be in the position of allowing itself to be persuaded by the NSA. Instead, the NSA would be dictating to NIST. This would violate the Act. As the decision to proceed with EES clearly comes from the highest levels of the U.S. government,[292] in the absence of firm information one cannot reject the deadlock scenario out of hand. There is, however, some reason to doubt it.

The deadlock scenario was anticipated in a 1989 codicil to the MOU.[293] After members and staff of the House Committee on Government Operations expressed concern about the apparent grant to the NSA of an effective veto over NIST's decisions, NIST and the NSA explained that although the Technical Working Group had broad jurisdiction as a discussion forum, the appeals process described in the MOU applied only to "proposed research and development projects in new areas."[294] This codicil, signed by representatives of both agencies with the express intent of binding their successors, distinguishes between "promulgation of standards and guidelines" by NIST, which are not subject to appeal,[295] and

---

officer properly and prudently followed the advice of the Comptroller General), *order aff'd*, 339 F.2d 753 (D.C. Cir. 1964).

[291] A deadlocked vote does not in itself require NIST to change its mind. Nevertheless, it is not difficult to imagine why an agency might choose to compromise rather than involve the head of the entire department in a battle with the Secretary of Defense. In any case, the MOU's involvement of the Secretary of Defense seems contrary to the Act because the Act envisions no decision-making role for anyone outside NIST. NIST is part of a chain of command that goes up through the Secretary of Commerce to the President. Both the President and the Secretary of Commerce are free to consult anyone in the Cabinet, if they desire, for advice, but the Act provides no authority for NIST to turn over actual decision-making power, even in shared form, to the Secretary of Defense.

[292] "The National Security Council, the Justice Department, the Commerce Department, and other key agencies were involved in this decision [to propose the Clipper Chip]. This approach has been endorsed by the President, the Vice President, and appropriate Cabinet Officials." Office of the Press Secretary, The White House, Questions and Answers About the Clinton Administration's Telecommunications Initiative 1 (Apr. 16, 1993), *in* "Key Escrow" Information Packet, *supra* note 20.

[293] *See* Letter from NIST and the NSA to the Hon. John Conyers, Jr. and the Hon. Frank Horton, House Comm. on Gov't Operations (Dec. 22, 1989), *reprinted in* OTA INFORMATION SECURITY, *supra* note 97, app. B at 201, 205-09.

[294] *Id.* at 206.

[295] *Id.* at 209.

the "early stage in the standards research and development process—usually years before a standard is promulgated,"[296] from which appeals are permitted.

Neither NIST nor the NSA have made public statements as to the involvement of the Technical Working Group in the decision to promulgate FIPS 185. Whether the agreement required NIST to refer EES to the Technical Working Group before issuing FIPS 185 is unclear. But it appears that under the distinction set out in the 1989 codicil to the MOU, FIPS 185 would have been within the jurisdiction of the Technical Working Group, but outside the appeals procedure. Thus, if the 1989 codicil controlled, the deadlock scenario could only have applied if NIST preferred an alternative to EES but was persuaded to use EES against its better judgment. Alternately, because SKIPJACK was developed by the NSA, it is entirely possible that the entire EES proposal originated in the NSA, and that by the time the NSA disclosed SKIPJACK to NIST, the NSA had decided that neither SKIPJACK nor EES was a "proposed research and development project[] in [a] new area[]" under the terms of the codicil.[297] Both NIST and the NSA assert that the appeals procedure has never been used.[298] The agencies contend that the lack of appeals is evidence of the success of their cooperation.[299] Whatever the facts, NIST owes the public, and Congress, a clearer explanation of its relationship with the intelligence community. Congress is entitled to an explicit reassurance that NIST remains in complete control of security for civilian federal computer systems as required by the Act. The House and Senate committees with oversight over NIST should force it to provide these assurances. If NIST is unable to do so because it has allowed its judgment to be suppressed by the NSA's veto, then Congress will need to revise the Computer Security Act to create stronger incentives for NIST to preserve its jurisdiction—perhaps even instituting penalties for noncompliance.[300]

---

[296] *Id.* at 208.

[297] *Id.* at 206.

[298] *See* OTA INFORMATION SECURITY, *supra* note 97, at 14.

[299] *See id.* at 14-15 (discussing the NSA's advisory role in working with NIST).

[300] *Cf. id.* at 16-18 (proposing seven options for congressional oversight and action on cryptography).

4. Who Should Hold the Keys?

The Administration does not intend to give the escrow agencies the sort of permanence or legal authority that derives from legislation, much less the autonomy that attaches to an independent agency or a nongovernmental actor.[301] This decision is very unfortunate given the crucial role that the escrow agents play in generating and safeguarding the keys. As ordinary administrative agencies within the executive branch, the escrow agents fall within the regular civilian chain of command and have no recourse if legally ordered to grant access to the keys to the NSA, the FBI, or future White House "plumbers." The heads of both escrow agencies serve at the pleasure of the President. The absence of any formal regulations that would impose delays, along with the absence of publicity as the rules are changed, prevents even a delaying action of the kind contemplated in *Nader v. Bork*[302] and *United States v. Nixon*.[303] Under current rules, the terms under which the escrow agents work can be modified, waived, or amended at any time without public notice, although the public might be able to find out about unclassified changes or waivers after the fact via the Freedom of Information Act.[304]

Ideally, the escrow agents would be as incorruptible as possible, possessed of a clear charter setting out their positive and negative duties, insulated from pressure from the law enforcement and intelligence communities, and outfitted with secure facilities to store the list of key fragments (which may, if EES catches on, become one of the most valuable items of information held by the U.S. govern-

---

[301] *See* Digital Privacy and Security Working Group, *supra* note 31, at 7 (critiquing guidelines set forth by the Clinton Administration for the Information Infrastructure Task Force).

[302] 366 F. Supp. 104, 108 (D.D.C. 1973) (holding that the Acting Attorney General violated Justice Department regulations in firing Watergate Special Prosecutor Archibald Cox without first changing the rules giving the prosecutor limited tenure in office or finding that Cox acted with "extraordinary impropriety").

[303] 418 U.S. 683, 697 (1974) (rejecting the argument that an action brought by a Special Prosecutor against the President was nonjusticiable because both parties were officers of the executive branch); *see* Michael Herz, United States v. United States: *When Can the Federal Government Sue Itself?*, 32 WM. & MARY L. REV. 893, 952-53 (1991) (noting the limited ability of the President to control executive and independent agencies). *See generally* Note, *Violations by Agencies of Their Own Regulations*, 87 HARV. L. REV. 629 (1974) (examining agencies' ability to depart from existing regulations).

[304] 5 U.S.C. § 552 (1988); *cf.* APA § 552(a)(2)(c) (1988) (requiring agencies to disclose changes in regulations that will affect such disclosures).

ment). They must also be trusted by the public, or the public will not participate in the EES scheme. With the exception of the secure facilities, the list of necessary attributes describes a body resembling the federal judiciary. Not surprisingly, some noted cryptologists have suggested that the judiciary hold the keys.[305] No doubt the judiciary could acquire the technical competence and equipment required to generate and secure the keys.

Whether judges could constitutionally hold one or more key fragments is a close question.[306] It is clear that Congress could not hold the keys, nor could any congressional agent.[307] Holding keys is an executive function. It would involve judges in the law enforcement process at a time when there is no case or controversy and, as regards the large majority of the keys, no prospect of one.

Because holding keys is an executive function, the judiciary (or an agency such as the Administrative Office of the U.S. Courts, which is responsible only to judges) can constitutionally hold the keys only if the function is "incidental" to its Article III functions.[308] If the task is more than "incidental," then the principle of separation of powers requires that it be undertaken by the executive branch or by private citizens.[309] The court taking

---

[305] *See, e.g.*, Silvio Micali, *Fair Public-Key Cryptosystems*, *in* ADVANCES IN CRYPTOLOGY—CRYPTO '92, at 113, 116 (Ernest F. Brickell ed., 1993).

[306] Others see the issues differently. *See, e.g.*, Letter from Johnny H. Killian, Senior Specialist American Constitutional Law, Congressional Research Service, to Joan D. Winston, Office of Technology Assessment 1 (March 3, 1994) (concluding that "placing custody of one of the keys in a federal court or in an agency of the Judicial Branch would almost certainly pass constitutional challenge"). In earlier drafts of this Article, I argued that holding keys was outside the judicial function because it was not "incidental" to any task specified in Article III. I am grateful to Larry Lessig and other participants in the LEXIS Counsel Connect on-line cryptography seminar for persuading me that there are two sides to the question.

[307] *See* Metropolitan Wash. Airports Auth. v. Citizens for the Abatement of Aircraft Noise, Inc., 501 U.S. 252, 276-77 (1991) (holding that the participation of members of Congress on a committee possessing the power to veto decisions regarding local airports violated the doctrine of separation of powers); Bowsher v. Synar, 478 U.S. 714, 727-32 (1986) (holding that the Comptroller General could not be considered an executive branch official because Congress reserved the right to remove him by legislation, and, therefore, he could not constitutionally exercise budget-cutting powers given to him by the Deficit Control Act); Buckley v. Valeo, 424 U.S. 1, 126-33 (1976) (holding that members of Congress could not constitutionally appoint the members of the Federal Election Commission).

[308] *See* Morrison v. Olson, 487 U.S. 654, 679 (1988) (stating that the Special Division may constitutionally exercise power to determine jurisdiction of Special Counsel only if this power is "truly 'incidental' to" its appointment power).

[309] *See id.* at 680-81 (noting that separation of powers ensures that "judges do not . . . undertake tasks that are more properly accomplished" by other branches).

custody of the keys would be in a position reminiscent of *Hayburn's Case*,[310] which has long stood for the proposition that neither the legislative nor executive branches may assign duties to the judiciary "but such as are properly judicial, and to be performed in a judicial manner."[311] Unlike *Hayburn's Case*, however, the judges would not be asked to decide anything until the government was granted a search warrant. The court would presumably disclose the key fragment(s) along with the ex parte order granting the warrant.

Judges already do a number of things that come close to holding a key fragment, but each is distinguishable. Courts and their adjuncts have for many years exercised a wide variety of ancillary powers such as rule making, and the appointment and supervision of court personnel, which are "reasonably ancillary to the primary, dispute-deciding function of the courts."[312] Courts have also supervised grand juries for many years.[313] More recently, Congress has given the judges and courts additional responsibilities, including membership on the Sentencing Commission,[314] and the selection and supervision of independent counsel.[315] Indeed, the granting of warrants (and the record-keeping which follows) are ex parte proceedings, clearly within the Article III jurisdiction of the courts. Taking custody of a key in advance of any adversary or even any ex parte proceeding, with the knowledge that most keys will never be subject to such a proceeding, goes beyond any of these precedents. Perhaps the closest analogy is the court's marshal who is instructed to keep order even though there is no reason to believe

---

[310] 2 U.S. (2 Dall.) 409 (1792).

[311] *Id.* at 410 n.† (reporter's note quoting from the judgment of the Circuit Court for the District of New York, a panel that included Chief Justice Cushing riding circuit); *see* United States v. Ferreira, 54 U.S. (13 How.) 40, 50-51 (1852) (relying on *Hayburn's Case*); *see also Buckley*, 424 U.S. at 123 (citing *Hayburn's Case* and *Ferreira* for the proposition that "executive or administrative duties of a nonjudicial nature may not be imposed on judges holding office under Article III of the Constitution"); National Mut. Ins. Co. v. Tidewater Transfer Co., 337 U.S. 582, 591 (1949) (Jackson, J., plurality opinion) (noting that courts properly are not asked to "participate in any legislative, administrative, political or other nonjudicial" functions).

[312] Chandler v. Judicial Council of the Tenth Circuit, 398 U.S. 74, 111 (1970) (Harlan, J., concurring in denial of writ).

[313] *See* Morrison v. Olson, 487 U.S. 654, 681 (1988) (discussing federal judicial control of the disclosure of federal grand jury matters).

[314] The membership of judges on the Federal Sentencing Commission was upheld against a separation of powers challenge in Mistretta v. United States, 488 U.S. 361, 371-412 (1989).

[315] The Supreme Court upheld the judiciary's role in the selection and supervision of independent counsel, in regards to the Ethics in Government Act of 1978, in *Morrison*, 487 U.S. at 684.

that any particular person will seek to disrupt the court's functioning. Even the marshals are an imperfect parallel, however, because their activities impinge only on persons who come into contact with the court or with court personnel; holding key fragments could affect the privacy of many who have no other contact with the judicial system.

Whether the functions of protecting keys from disclosure and disclosing keys to facilitate wiretaps are sufficiently ancillary to the judicial function of issuing wiretap orders and warrants as to be constitutional is ultimately a matter of taste. The existence of the FISA court,[316] whose sole jurisdiction is to receive and rule on petitions for foreign-intelligence-related surveillance, adds some support to the argument that holding a key fragment would be incidental to Article III functions, because the act of holding the keys is only a little more ancillary to traditional judicial functions than are the FISA court's actions.[317]

As a quick fix, the Secretary of Commerce and the Secretary of the Treasury should each immediately issue separate regulations, published in the *Federal Register*, defining the role of the escrow agents in their respective agencies and making clear that the escrow agents have a legal duty to protect the keys from all release except as specified in the rules. In the longer term, Congress should pass legislation vesting the escrow function in independent agencies specifically created for that purpose.[318] Although opinions differ as to the degree of tenure in office that the Constitution allows Congress to confer on the heads of independent agencies,[319] there

---

[316] *See* 50 U.S.C. §§ 1801-1811 (1988); *see also supra* note 196 and accompanying text.

[317] *See* Letter from Johnny H. Killian to Joan D. Winston, *supra* note 306, at 1-3 (discussing the probable constitutionality of placing custody of keys in the federal judiciary).

[318] The proposed "Encryption Standards and Procedures Act of 1994" falls far short of this objective because it allows the President to designate any technologically qualified agency to hold key segments, so long as such agency lacks the authority to conduct wiretaps. *See* H.R. 5199, *supra* note 218, § 31(d)(1)-(2).

[319] *Compare* Steven G. Calabresi, *The Vesting Clauses as Power Grants*, 88 NW. U. L. REV. 1377, 1389-1400 (1994) (describing the unitary executive theory, which suggests that there is only limited congressional power to restructure the executive department because the President is vested with the power to control and direct subordinate officials in their execution of statutory provisions) *and* Steven G. Calabresi & Kevin H. Rhodes, *The Structural Constitution: Unitary Executive, Plural Judiciary*, 105 HARV. L. REV. 1155, 1155-71 (1992) (same) *and* Kevin H. Rhodes, *A Structure Without Foundation: A Reply to Professor Froomkin*, 88 NW. U. L. REV. 1406, 1416-17 (1994) (same) *with* A. Michael Froomkin, *The Imperial Presidency's New Vestments*, 88 NW. U.

is no debate that independent agency status represents an attempt to shield a function from political manipulation, and that the officers of an independent agency have at least political insulation from dismissal by a President who finds them insubordinate.

Alternate structures, in which EES-product users can choose to lodge their keys with any one of a number of private escrow agents, might provide even greater security to users, but at the price of some additional complexity. One can imagine a system in which private escrow agents would apply to the Attorney General for certification as suitably secure and perhaps post bond to ensure that they would deliver up keys when legally ordered to do so. Although this system might satisfy both the user's desire for security and the government's desire for certain access, it introduces practical problems. The government will still need to keep a master list of chip serial numbers in order to know which escrow agent has the key. Furthermore, a private escrow agent would have to charge a fee, to be paid either by the chip user or the taxpayer. There is also no particular reason to believe private escrow agents would be less corruptible than the Justice Department, although if key fragments were distributed among many different escrow agents, the harm caused by compromise of any given database would be lessened.[320]

B. *Unresolved Issues*

In testimony to the haste with which the Administration launched the EES program, important implementation issues remain unresolved.

L. REV. 1346, 1347-49, 1366-69 (1994) (arguing that the Constitution gives Congress broad power to structure the President's control over the executive department) *and* A. Michael Froomkin, *Still Naked After All These Words*, 88 NW. U. L. REV. 1420, 1427-30 (1994) (same) *and* A. Michael Froomkin, Note, *In Defense of Administrative Agency Autonomy*, 96 YALE L.J. 787 (1987) (same).

[320] Even more complex, and elegant, solutions exist. *See, e.g.*, Silvio Micali, Fair Cryptosystems 7-8 (Aug. 1994) (unpublished manuscript, on file with author). Micali proposes a scheme in which the key can be broken up into any number of parts, and in which every part of the key is required to decrypt the message. *See id.* at 7. Micali's scheme includes a number of elegant but complex refinements, notably a scheme for making the keyholder "oblivious." *Id.* at 18, 40-41. By "oblivious" Micali means that even the trustee need not know the identity of the person whose key has been requested by the government. *See id.* at 18. In this way the trustees are unable to notify the person whose communications are being wiretapped. *See id.*

1. Requests From Foreign Governments

The National Security Council is currently considering under what circumstances, if any, foreign governments would be given the U.S. family key.[321] What if, for example, Great Britain, a friendly government, wished to decrypt a conversation in which someone had used a Clipper-equipped telephone to place a call from London to New York, or from Paris to London? Or suppose a friendly foreign government stated that it would outlaw the use of Clipper-equipped telephones unless it were given the family key and promised that requests for specific chip keys would be honored?[322] At the moment, no policy exists to answer these questions. Giving a foreign government the family key puts it one step closer to decrypting all Clipper traffic; this weakens the security that Clipper is supposed to provide.[323] Refusing to share information with foreign law enforcement and intelligence agencies risks disrupting working relationships. Even a compromise solution, in which the U.S. offers to decrypt messages on a case-by-case basis, might be unpopular both with Clipper users and foreign governments. Indeed, some intelligence-sharing treaties may require either that the tools for decrypting EES traffic be shared with some foreign intelligence agencies, or that the U.S. do the decryption on demand.[324]

The proposed Encryption Standards and Procedures Act would have authorized the President to release keys to foreign governments when she "determines that such access and use is in the

---

[321] *See* Telephone Interview with Lynn McNulty, Associate Director, NIST (Aug. 5, 1994).

[322] France, for example, prohibits the use of unregistered cryptographic algorithms. *See* JAMES P. CHANDLER, ET AL., NATIONAL INTELLECTUAL PROPERTY LAW INST. & GEORGE WASHINGTON UNIV., IDENTIFICATION AND ANALYSIS OF FOREIGN LAWS AND REGULATIONS PERTAINING TO THE USE OF COMMERCIAL ENCRYPTION PRODUCTS FOR VOICE AND DATA COMMUNICATIONS § 2.7.1 (Jan. 1994).

[323] Recall that, according to the FBI, industrial espionage by friendly foreign governments is a growing threat to U.S. businesses. *See supra* note 43 and accompanying text.

[324] The NSA has long-standing and close relationships with some of its foreign counterparts. *See* BAMFORD, *supra* note 17, at 309-37 (discussing BRUSA and UKUSA agreements with UK, Canada, Australia). The texts of the agreements, which date back to 1947, remain classified. John Gilmore has filed a FOIA request seeking information as to these agreements. *See* Posting from John Gilmore to USENET Group sci.crypt (Dec. 10, 1993) (on file with author). The NSA has yet to provide significant documents in response to this request. *See* Telephone Interview with Lee Tien (July 27, 1994) (notes on file with author) (Tien represents Gilmore in his FOIA request).

national security and foreign policy interests of the United States."[325] Nothing in the draft legislation would have required that the owner of the chip ever be notified that her security has been permanently compromised. It is interesting to speculate whether a company that suffered a loss due to the release of commercially sensitive information in this manner would have a takings or a tort claim against the United States.

2. Clipper Abroad?

Unlike other modern encryption products, Clipper-equipped products will be exportable. Presumably, U.S. businesses using Clipper at home will welcome the opportunity to use the same products in their foreign subsidiaries. Whether other foreigners would wish to buy a product that comes with a guarantee that the U.S. government can listen in seems more doubtful.

There are two strategies, however, that the Administration might use to boost foreign sales. The first would be to share the family key with foreign governments and perhaps also allow those governments to be the escrow holders for certain chips. The alternative would be to manufacture some chips with a different family key, perhaps even a different family key for each foreign market. The alternative family key could be disclosed to the foreign government without compromising the security of the U.S. chips, but two chips with different family keys would not be able to communicate in secure mode because they would not recognize each other's LEAFs as valid.

The globalization of commerce means that sensitive commercial (and, increasingly, personal) communications cross national borders. Even if EES becomes the de facto U.S. standard, it is unlikely to meet with wide acceptance abroad as long as the family key and the chip unique keys are held by the U.S. government. Why, after all, should non-U.S. buyers acquire a product designed to make eavesdropping by the U.S. government relatively easy?[326] Whether

---

[325] H.R. 5199, *supra* note 218, § 31(e)(2)(B).

[326] One newspaper reported as follows:

> The US plan for a Clipper chip . . . has raised fears among European businesses that sensitive information would no longer be secret if it were vetted by the CIA [or] the FBI . . . .
>
> . . . .
>
> . . . [T]he European organisation representing users of computer security has rejected the Clinton initiative as "totally unacceptable."

non-U.S. buyers choose a similar product with a different family key or a different system entirely, the result will be to make secure communications between a U.S. party and a non-U.S. party more difficult. If, as the FBI suggests, the U.S. has the most to lose from industrial espionage,[327] EES may hurt U.S. business more than it hurts anyone else.

3. What Level of Protection Do LEAFs Have Under the Electronic Communications Privacy Act?

The contents of an ordinary conversation on the telephone, even one that is not encrypted, are a "wire communication" and hence entitled to the highest statutory protection provided by Title III, as well as the full protection of the Fourth Amendment. It is clear that an encrypted voice communication, even one digitized by a Clipper Chip, remains a "wire communication" for Title III purposes.[328] By contrast, an "electronic communication"—digitized data—receives a lower level of statutory protection, although it is still illegal to intercept it without a judicial order, and the Fourth Amendment still applies with full force. A LEAF on its own, without a conversation following it, would only be an electronic communication, not a wire communication.[329]

A LEAF followed by a wire communication presents a complicated problem under the Electronic Communications Privacy Act of

---

> . . . [T]he Information Security Business Advisory Group (Ibag), warns European governments to ignore overtures from the US government aimed at restricting access to the information superhighway to users who use encryptions that the government agencies can decode.

Leonard Doyle, *Spooks All Set to Hack It on the Superhighway*, INDEPENDENT (London), May 2, 1994, at 10.

[327] *See supra* note 43 and accompanying text.

[328] *See* S. REP. NO. 541, 99th Cong., 2d Sess. 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 ("The conversion of a voice signal to digital form for purposes of transmission does not render the communication non-wire."). A wire communication is an "aural transfer" made in whole or in part by wire, cable, or other like connection (for example, a telephone call). 18 U.S.C. § 2510(1) (1988). "Aural transfer" means "a transfer containing the human voice at any point between and including the point of origin and the point of reception." § 2510(18).

[329] The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510-2521 (1988 & Supp. V 1993)), defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but . . . not includ[ing] . . . any wire or oral communication." 18 U.S.C. § 2510(12).

1986 (ECPA).[330] The sensible argument that the LEAF is an integral part of the conversation, and thus really within the umbrella of the wire communication that follows, hits a snag due to the ECPA's definition of the "contents" of a wire communication. Where formerly Title III had defined the contents of a wire communication as including any information "concerning the identity of the parties to such communication,"[331] the ECPA deleted the quoted words, leaving the contents of a wire communication defined as only the "substance, purport, or meaning" of the communication.[332] Fitting a LEAF within that definition requires a stretch. The LEAF itself contains none of the "substance, purport, or meaning" of the encrypted conversation—just information about the identity of the chip needed to acquire those things.

If a LEAF were found to be an electronic noncommunication legally severable from the wire communication that follows it, the LEAF would enjoy a lower level of statutory protection than if the LEAF were treated as part of the content of the wire communication: (1) Law enforcement officials would not need a warrant to intercept and record a LEAF, but only the more routine judicial orders required for pen registers;[333] (2) under the ECPA, any Assistant U.S. Attorney would be allowed to seek a court order to intercept a LEAF, not just the specially designated high-ranking members of the Justice Department who have authority to seek a wiretap warrant;[334] and (3) the statutory exclusionary rule applicable to wire communications would not apply.[335] Without the

---

[330] A LEAF followed by an e-mail does not present the statutory problem discussed in this subsection because both the LEAF and the e-mail are electronic communications under 18 U.S.C. § 2510(12). The Fourth Amendment analysis, however, does apply to a LEAF preceding an e-mail message.

[331] 18 U.S.C. § 2510(8).

[332] *Id.*

[333] *See* FISHMAN SUPPLEMENT, *supra* note 199, § 7.3.

[334] *See id.* § 42.1 (Supp. 1993). This difference is more significant than it may sound. *See* United States v. Giordano, 416 U.S. 505, 524-29 (1974) (holding that warrant application initialed by Attorney General's executive assistant, apparently without the Attorney General's knowledge, was invalid).

[335] The statutory exclusionary rule appears at 18 U.S.C. § 2515; *see also* § 2511(1)(d) (making it unlawful to use the contents of any wire or oral communication obtained in violation of the statute). Unlike the constitutional exclusionary rule, the statutory rule reaches private action, applies in civil and regulatory proceedings as well as in criminal cases, and is unaffected by the growing body of exceptions the Supreme Court has placed on the constitutional exclusionary rule, such as good faith exceptions, the eventual discovery exception, and the exception for use in rebuttal. *See* § 2515. I am indebted to Charles C. Marson for pointing this out to me.

statutory exclusionary rule, the victim of an illegal interception of a LEAF would have a civil remedy (and the interceptor would face possible criminal prosecution), but no right to suppress evidence would exist unless the Fourth Amendment's exclusionary rule applied.[336]

If a LEAF is severable in this manner, it is not as clear as it should be that the LEAF would enjoy any protection under the Fourth Amendment. Because decrypting the LEAF with the family key involves listening to at least a few seconds of the conversation, the act of intercepting and decrypting the LEAF is a wiretap of an electronic communication even if the information thus gathered (the identity of the other chip) is no greater than could be had with a trap and trace or a pen register. Traffic analysis using pen registers (which record the numbers called by a telephone) and trap and trace devices (which record numbers calling the telephone) does not implicate the Fourth Amendment.[337] Under Title III, however, both methods require a court order, although an actual warrant is not required.[338] Despite being a wiretap, the interception of a LEAF might not violate the Fourth Amendment if the telephone user has no reasonable expectation of privacy for the LEAF.

An EES chip user should have a reasonable expectation of privacy, as the term is used in Fourth Amendment cases,[339] in her LEAF, but the question is not as free from doubt as it should be. The difficulty arises because the user is aware that the government has the information needed to decrypt the LEAF. Although the government has promised to use that information only in specific circumstances, it is just a promise, and as the government cannot be estopped, it is usually free to renege, although in some circumstances this action might amount to a denial of due process.

---

[336] *See* § 2520 (providing for damages and injunctive relief in civil actions). Congress deliberately omitted an exclusionary remedy. *See* S. REP. NO. 541, *supra* note 328, at 23, *reprinted in* 1986 U.S.C.C.A.N. at 3577; FISHMAN SUPPLEMENT, *supra* note 199, §§ 252.1, 253. I am again indebted to Charles C. Marson for pointing this out to me.

[337] *See supra* note 211.

[338] *See* 18 U.S.C. §§ 3121-3123 (1988); *supra* note 211.

[339] *See, e.g.*, United States v. Miller, 425 U.S. 435, 442-43 (1976) (holding that by voluntarily conveying information to a bank and its employees, the respondent did not have a legitimate expectation of privacy); Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth . . . .").

A reasonable expectation of privacy requires both a subjective expectation of privacy and an "objective" recognition that the expectation is reasonable.[340] A Supreme Court that can hold that one has no reasonable expectation of privacy in the telephone numbers one dials,[341] or in the checks one allows to be cleared by one's bank,[342] because the information has been disclosed to others, is capable of holding that emitting a LEAF with knowledge that the government can decrypt it puts the LEAF in the same position as the telephone number dialed.[343]

A LEAF on its own is not worthless, although it is worth less than a session key. A large-scale eavesdropper armed with the family key could collect LEAFs. Because each LEAF contains the chip serial identifier, it allows a large-scale eavesdropper to conduct traffic analysis[344] without having to gain access to a telecommunication provider's equipment to set up thousands of trap and traces or pen registers. If satellite or microwave telephone signals are being monitored, the LEAF-monitoring method of traffic analysis is undetectable.[345] Furthermore, if one is trying to collect all the calls from a particular machine in an attempt to decrypt them, decrypting the LEAF allows one to know which calls to record and file for future reference. Of course, if the eavesdropper has a warrant, in most cases all of this and more is easily obtained from the telephone service provider.[346] It would be monstrous, though, to have a rule that said the government could acquire the LEAF for traffic analysis after falsely promising the American people that EES

---

[340] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[341] *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

[342] *See Miller*, 425 U.S. at 443 (holding that a depositor had no legitimate expectation of privacy, and hence no protectable Fourth Amendment interest, in copies of checks and deposit slips retained by his bank because the depositor, by writing the checks and making the deposits, had taken the risk that "the information [would] be conveyed . . . to the Government").

[343] For an argument that *Miller* should be reversed on the theory that the Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §§ 3401-3422 (1988 & Supp. V 1993)), creates a reasonable expectation of privacy in bank records, see Bercu, *supra* note 90, at 407-09.

[344] *See supra* text accompanying note 155 (noting that intelligence agencies learn important information by tracking who calls whom).

[345] Because telephone traffic carries with it switching information regarding the destination of the call (information that is used by the service provider's routing system), a sophisticated eavesdropper may in any event have access to some of this information with less effort.

[346] *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 103(a)(1), 108 Stat. 4279, 4280 (1994) (requiring telephone-service providers to make systems wiretap-ready).

would be secure. A court construing both the objective and subjective prongs of the reasonable expectation of privacy test would have a moral obligation to take this into consideration.

C. *Voluntary EES Is Constitutional*

Even if EES is unreasonable either on general principles or as the term is used in the context of the APA, it is still not unconstitutional. The Constitution allows many unreasonable things,[347] and actions that might violate the APA if made by rules within its purview are not necessarily unconstitutional if achieved by other means. So long as it remains purely voluntary, EES creates no fundamental constitutional problems.

EES involves five distinct government actions. First, the government launched the program by making the classified SKIPJACK algorithm available to a manufacturer of EES-compliant products. Second, the government announced FIPS 185.[348] Third, it is purchasing large numbers of EES-compliant products for its own use. Fourth, it is encouraging others to use EES products. Fifth, it is setting up the two escrow agents who will hold the keys. As a group, these five actions amount to attempting to create a voluntary national key escrow system. Individually and collectively these activities are constitutional.

The NSA controls access to the SKIPJACK algorithm and the details of the LEAF.[349] To date it has made the design of the chips available to one manufacturer, Mykotronx, Inc.[350] FIPS 185 indicates that only organizations already holding security clearances need apply for access to the classified specifications for SKIPJACK. A party lacking such a clearance might have a legitimate grievance if she were unable to obtain such clearance for the purpose of

---

[347] *See, e.g.*, Corn Exch. Bank v. Coler, 280 U.S. 218, 223 (1930) (allowing seizure of absconding husband's property without prior notice); Henry P. Monaghan, *Our Perfect Constitution*, 56 N.Y.U. L. REV. 353, 396 (1981) (arguing that, contrary to arguments of "due substance" theorists, the Constitution does not protect some external concept of morality and does not guarantee perfect government).

[348] The legal issues raised by publication of FIPS 185 are discussed above, *see supra* parts II.A.1-3, and will not be repeated here.

[349] *See* FIPS 185, *supra* note 14, at 6004 ("The National Security Agency maintains these classified specifications and approves the manufacture of devices which implement the specifications.").

[350] The only members of the public who have had access to the inner workings of SKIPJACK are a committee of five outside experts who were asked to examine SKIPJACK so that they could opine on its security. *See* SKIPJACK Interim Report, *supra* note 187.

manufacturing EES-compliant microcircuitry.[351] Indeed, if potential competitors to the NSA's chosen manufacturer were denied access to the information they needed to compete with Mykotronx, they could plausibly allege an equal protection violation or a violation of procedural due process. The government has no obligation, however, to make the algorithm available to anyone who asks.[352]

The government is free to purchase goods and services to meet its needs.[353] Choosing to purchase EES-compliant devices does not, in itself, create any constitutional issues. Such purchases are constitutional even if they work as an indirect subsidy to producers who are able to lower their unit costs. The government could constitutionally provide direct subsidies if Congress chose to do so.[354] Nor is the denial of market share to non-EES products unconstitutional, even if it has the effect of raising their costs.

The government's cheerleading for EES is also constitutionally permissible. So long as no one is threatened with sanctions for failing to adhere to EES, the government is entitled to make its case to the nation for why we would all benefit if we accepted a limit on our privacy.[355]

---

[351] *See, e.g.*, Greene v. McElroy, 360 U.S. 474, 508 (1959) (holding that absent explicit authorization from either the President or Congress, an executive agency may not create a security program that deprives a civilian of employment without an opportunity to challenge an adverse determination of security clearance); Adams v. Laird, 420 F.2d 230, 235, 238-39 (D.C. Cir. 1969) (finding no due process violation when an applicant for security clearance is afforded a noncustodial interview and is able to cross-examine witnesses supplying adverse testimony, and when the agency follows clearly enunciated standards and makes adequate findings with respect to such standards), *cert. denied*, 397 U.S. 1039 (1970).

[352] *See, e.g.*, 18 U.S.C. § 793 (1988) (criminalizing the unauthorized disclosure of cryptographic information).

[353] *See, e.g.*, Reeves, Inc. v. Stake, 447 U.S. 429, 439 n.12 (1980) (describing the government's "'unrestricted power . . . to fix the terms and conditions upon which it will make needed purchases'" (quoting Perkins v. Lukens Steel Co., 310 U.S. 113, 127 (1940))).

[354] Congress thus far has made no such choice in this case. Congress has given the Attorney General discretion to spend monies in the Asset Forfeiture Super Surplus Fund. *See supra* note 244 and accompanying text (describing the Fund). Conceivably, a court might imply a limit to this delegation and might find that the attempt to determine industrial policy in its use of the Fund exceeded the implicit limit. Because there appears to be no one with standing to sue, this must remain speculation.

[355] *See* Meese v. Keene, 481 U.S. 465, 479-80 (1987) (holding that government labeling of environmental films as "political propaganda" is permissible government speech); THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 699-708 (1970) (stating that government has the same freedom of speech as individuals);

The government has the authority to act as an escrow agent,[356] although there is some question from where the money to pay for the escrow agents would come. Preliminary estimates put the cost of the escrow agents' activities at $16 million per year.[357] These expenses may require a separate appropriation by Congress, although both NIST and the Justice Department have funds which arguably might be tapped for this purpose.[358]

Nor is the program as a whole unconstitutional. Even if EES becomes widespread, everyone in the U.S. remains free to use any alternative, subject only to restrictions on his or her ability to export the cryptosystem to foreign correspondents.[359] It remains feasible and legal to preencrypt a message with an ordinary, non-escrowed cipher, feed it to an EES-compliant device, and make even EES communications potentially unintelligible to eavesdroppers armed with the chip unique key.[360] Indeed, the very ease with which EES

MARK G. YUDOF, WHEN GOVERNMENT SPEAKS: POLITICS, LAW, AND GOVERNMENT EXPRESSION IN AMERICA 301 (1983) (stating that courts "create more problems than they solve" when they attempt to limit government expression); Steven Shiffrin, *Government Speech*, 27 UCLA L. REV. 565, 622 (1980) (encouraging application of a balancing test when analyzing government subsidies such as election funding and free speech); Mark G. Yudof, *When Governments Speak: Toward a Theory of Government Expression and the First Amendment*, 57 TEX. L. REV. 863, 917 (1979) (arguing for legislative rather than judicial control of government speech); *cf.* Beth Orsoff, Note, *Government Speech as Government Censorship*, 67 S. CAL. L. REV. 229, 234 (1993) ("[A]ll government criticism carries with it an implied threat. Thus, the test should be whether the average reasonable person receiving the government criticism would perceive it as a threat, not whether the government official can legitimately execute the threat."). By this standard, cheerleading for Clipper seems to be permissible, although I have qualms about speaking for "the average reasonable person." If, however, the government pressured AT&T into abandoning its plans to manufacture a DES-based secure telephone and to substitute a Clipper telephone instead, then the cheerleading stepped over the line to impermissible coercion.

[356] *See, e.g.*, 15 U.S.C. § 272(c)(22) (1988) (catchall provision for authorized NIST activities).

[357] *See* FIPS 185, *supra* note 14, at 6000.

[358] The Justice Department has available the Asset Super Surplus Forfeiture Fund. *See supra* note 244 and accompanying text (describing the Fund). NIST has a cost recovery fund and a working capital fund. *See* 15 U.S.C. § 278b (1988).

[359] *See supra* text accompanying note 165 (discussing the prohibition of the export of cryptographic software and hardware).

[360] Preencrypting a message with an ordinary, non-escrowed cipher, then feeding it to an EES-compliant device preserves the user's ability to make it appear that the message complies with EES while, in fact, partially subverting it. A casual inspection of the message will reveal a valid LEAF, and decrypting the LEAF with the family key will reveal a valid chip serial number. Decrypting the message with the session key obtained from the escrow agents, however, will reveal nothing more than a new ciphertext. Eavesdroppers remain able to do traffic analysis by logging the serial numbers of chips as they communicate, but they cannot hear or read the message

can be circumvented raises the possibility that the government might some day require key escrow as the price of using strong cryptography.

D. *Voluntary EES Is Unlikely to Displace Un-Escrowed Cryptography*

As we have seen, the Administration's stated motives for EES are not entirely consistent. The government's "hard sell" depicts non-EES encryption as a threat that needs to be avoided.[361] By contrast, the "soft sell" treats EES as part of a package deal that the government offers to those who desire government-certified encryption.[362] EES is officially voluntary, yet has been introduced in a manner which the government hopes will induce, even coerce, the public to choose an EES system over any alternative.[363] In the Administration's view, it is unreasonable to object to a plan that protects users from communications interception by everyone except the government. At worst, the Administration argues, under EES the user bears no greater risk of government interception (authorized or not) than do unencrypted callers.[364] Supporters also point to the need to help law enforcement in the fight against dangers such as terrorism.[365]

Perhaps the most often repeated objection to EES is that because people remain free to use alternatives, EES can never achieve its stated objective of maintaining law enforcement access to private encrypted communications. Clipper's critics suggest that it can catch only stupid criminals. The government has had three responses to this argument. The least subtle response has been that

---

without cracking the additional cipher.

FIPS 185 prohibits the *post*encryption of an EES message. Because FIPS 185 is only a nonbinding standard, it remains legal to postencrypt output from a Clipper or Capstone Chip, making the LEAF unintelligible to even a public servant armed with the family key. Although it is legal, it is also fairly pointless: if you are going to use another system on top of Clipper/Capstone, why bother using the latter at all? Because postencryption violates FIPS 185, an EES-compliant device will refuse to decrypt a postencrypted message, making postencryption of limited utility.

[361] *See supra* text following note 139; *supra* text accompanying note 152.

[362] *See supra* text accompanying note 141.

[363] *See supra* text accompanying notes 242, 246.

[364] Although forceful, this argument ignores the difference between illicit government surveillance that requires an intrusion into the home or office, and illicit surveillance that does not. If the White House "plumbers" who committed the Watergate burglary had been able to wiretap the Democratic National Committee from the outside, there would never have been a "third-rate burglary" detected by an alert security guard, and President Nixon would have completed his second term.

[365] *See supra* text accompanying note 143.

criminals are often dumber than one thinks.[366] A more subtle response is that Clipper may at least postpone the perhaps inevitable adoption of an alternative cryptosystem that the government cannot easily decrypt.[367] The most subtle response notes that a secure communication requires compatible equipment on both ends of the line.[368] If Clipper becomes the de facto standard, the existence of a few other devices on the margin will have a negligible effect on the government's ability to monitor electronic communication when it feels required to do so.

The government's policy centers on its hope that EES will become the market standard. Yet EES will not likely triumph in the marketplace, even with the advantage of massive government orders, because many people find something deeply distasteful about being asked to buy a product that comes ready-made to be wiretapped, even if the wiretapping is designed to be conducted only in limited circumstances by duly authorized bodies. In light of likely technical developments, a "threat assessment" of the government's potential surveillance capabilities makes the thought of wiretap-ready communications even more disturbing. This is especially true considering the history of government abuse of civil rights and the possibility, however remote, that government policy might change even as escrowed chip keys remain fixed. In any case, for e-mail, alternatives to EES already exist which are cheaper, more flexible, and appear to offer more complete privacy.[369] Non-EES

---

[366] "You shouldn't over estimate the I.Q. of crooks." Stewart A. Baker, Data Encryption: Who Holds the Keys?, Address Before the Fourth Conference on Computers, Freedom and Privacy 8 (Mar. 24, 1994) (transcript on file with author) [hereinafter Baker Talk]. Indeed, criminals often use ordinary telephones, which can be wiretapped.

[367] As Stewart Baker, then the General Counsel of the National Security Agency, put it:

> The concern is not so much what happens today when people go in and buy voice scramblers; it is the prospect that in five years or eight years or ten years every phone you buy that costs $75 or more will have an encrypt button on it that will interoperate with every other phone in the country and suddenly we will discover that our entire communications network, sophisticated as it is, is being used in ways that are profoundly anti-social. That's the real concern, I think, that Clipper addresses. If we are going to have a standardized form of encryption that is going to change the world we should think seriously about what we are going to do when it is misused.

Id. at 9.

[368] *See* Denning, *supra* note 206, at 322.

[369] *See supra* note 73 and accompanying text (describing how to get military-grade cryptography on the Internet).

voice products are also becoming available.[370]

1. Why EES Worries People

In addition to the fundamental objection that the government should not expect Americans to facilitate the decryption of their private communications, opponents of EES have raised numerous technical and practical objections to the plan. Critics of EES take what appears to the government to be an absolutist stand, refusing to trust anyone with the key needed to decrypt their communications.[371] To these critics, the government's protestation that EES adds nothing to current authority because federal law enforcement agencies need the same court order to obtain a wiretap on an EES-equipped phone as on an ordinary telephone, makes no impression. The critics believe either that current rules provide insufficient privacy or that the government cannot be trusted to follow the rules.

a. *Preserving the Status Quo Prevents a Return to the Status Quo Ante*

The status quo that EES seeks to preserve was not always the status quo. At the time Americans adopted the Bill of Rights, private communications were far more secure than they are today. Before the invention of the telephone, the radio, and the long-distance microphone, one could have a secure conversation by going for a quiet walk in an open field. Correspondents could encrypt letters in ciphers that no government could break.[372] Modern

---

[370] A program called AquaFone (so named because the imperfect voice quality makes it sound as if the user is speaking under water) is now available from Cogon Electronics of Culpeper, Virginia. The program uses RSA encryption under license from RSA Data Security, Inc., and sells for $129. The hardware requirements are minimal, as the two parties to the conversation need only a personal computer, a sound card, and a modem. The company markets a demonstration disk via its 800 number.

Phil Zimmermann, the creator of the popular shareware encryption program PGP, and a development team are currently working on a voice version of the PGP encryption program, nicknamed "Voice-PGP." The program will be released early in 1995, although the actual name has not yet been selected. *See* Telephone Interview with Philip Zimmermann (Dec. 6, 1994) (notes on file with author).

[371] The classic line, now almost a battle cry, is John Barlow's proclamation, "[Y]ou won't pry my fingers from its private key until you pull it from my cold dead hands." Steven Levy, *Crypto Rebels* (June 1994), *available online URL* http://wwn.cggnus.com/~gnu/crypto.rebels.html.

[372] The Vigenère cipher, which was well-known by the 17th century, was still considered unbreakable at the time of the American Revolution. *See* KAHN, *supra*

communications have expanded the circle of people to whom we speak, but this fact alone does not mean that communications should necessarily be more vulnerable. Only recently, it was difficult for the government to trace incoming calls, even pursuant to a court order, because the telephone company used slow mechanical tracing devices. Having overcome that problem, the FBI now seeks legislation to keep it from becoming difficult again.[373] Nor does the possibility that more criminals will avoid detection if the privacy available to individuals were to be increased necessarily mean that choosing to increase privacy is unwise. The Bill of Rights already includes many provisions that prefer to provide protections to all citizens at the cost of providing benefits to the guilty.[374] What this means is that some value judgments must be made, and that someone will have to make them.

Where once people only had to worry about eavesdroppers they could see, today an eavesdropper could be anywhere that a telephone signal happens to reach. Modern encryption seems

---

note 6, at 214-21. Indeed, *Scientific American* wrongly described the cipher as uncrackable as late as 1917. *See id.* at 148. For a fascinating discussion of Thomas Jefferson's creation of a cryptosystem still good enough to be used by the U.S. Navy in 1967, see *id.* at 192-95.

[373] *See* Nelson, *supra* note 138, at 1139-42 (describing preliminary draft of digital telephony legislation, requiring the alteration of electronic communications equipment to enable the government to maintain its current wiretapping capabilities).

[374] The individual's right to remain silent harms the prosecution; England recently abridged the right for that reason. *See* Criminal Justice and Public Order Act, 1994, ch. 33, §§ 34-37 (Eng.) (providing that courts may draw adverse inferences from the silence of suspects). As a result of this legislation, the warning to be given to suspects upon arrest has been tentatively redrafted to read:

> You do not have to say anything. But if you do not mention now something which you later use in your defence the court may decide that your failure to mention it now strengthens the case against you. A record will be made of anything you say and it may be given in evidence if you are brought to trial.

Jason Bennetto, *New Police Caution Alarms Legal Experts*, INDEPENDENT (London), Aug. 20, 1994, at 4 (quoting the draft text of the revised caution to suspects). Whether this change will ever take effect—or survive judicial review if it does—is open to question because the European Court of Human Rights recently ruled that the right to remain silent is guaranteed under the European Convention on Human Rights (formerly known as the Convention for the Protection of Human Rights and Fundamental Freedoms), Nov. 4, 1950, art. 6(1), 213 U.N.T.S. 221. *See* Funke v. France, 256 Eur. Ct. H.R. (ser. A) at 8 (1993) (holding that Article 6(1) of the European Convention on Human Rights guarantees the right against self-incrimination); Ying H. Tan, *Use of DTI Interviews Unfair*, INDEPENDENT (London), Sept. 30, 1994, at 30 (reporting the decision of the European Commission of Human Rights in *Saunders v. United Kingdom*).

poised to re-create the functional equivalent of the privacy available in the late 1790s and to apply it to devices like telephones and modems, which are increasingly replacing face-to-face contact and letter writing.[375] EES would prevent this return to the status quo ante, at least when the government is the eavesdropper.

Widespread adoption of Clipper and massive wiretapping ability would make traffic analysis more feasible for a hypothetical government oblivious to the need to obtain warrants. If Clipper is widely used, communications encrypted by other means signal that the user may have something to hide. Indeed, for this reason some privacy advocates encourage the routine use of strong cryptography in all communications in order to provide a cloaking effect for all personal communications. If everyone makes a habit of using strong cryptography, the presence of an encrypted message will never be probative of a guilty conscience or a need for secrecy.[376]

b. *EES Does Not Preserve the Status Quo*

EES is designed to be inflexible, and this inflexibility will impose costs on some users. Each chip's unique key is permanently branded onto it. If for some reason that key should be compromised, the user has no choice but to throw away the chip and buy a new one. This inflexibility is designed to make it impossible for users to select keys that are not held by the government.[377] Under Title III, the government must notify persons who were the subject of an authorized wiretap.[378] This duty is unaffected by EES, but

---

[375] The important difference between the 18th and 20th centuries is that rapid communication is possible over much greater distances.

[376] *See, e.g.*, *PGP™ User's Guide*, *supra* note 73 (maintaining that the encryption habit increases the supply of privacy, a public good, to everyone).

[377] "It is very important to change keys frequently to minimize" the problem of key compromise. SCHNEIER, *supra* note 12, at 27. In a software-based cryptographic system, changing the key is as easy as pressing a button. The Clinton Administration has repeatedly said that it would be pleased to consider software-based escrow systems if they could be designed in a way that prevented users from using non-escrowed keys.

[378] *See* 18 U.S.C. § 2518(8)(d) (1988) (requiring that "[w]ithin a reasonable time but not later than ninety days after" the termination of a wiretap, the persons named in the wiretap order and "such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice," must be given notice of the wiretap and of the fact that communications were intercepted; and providing that upon the filing of a motion, the judge has discretion to allow access to such portions of the intercepted communications for inspection as the judge believes to be warranted by the interests of justice).

the consequences change. Previously there was little a citizen needed to do after receiving notice that her phone had been tapped, but now she must consider whether the disclosure to law enforcement officials of the chip unique key in her telephone means that she should replace it, at a cost,[379] or whether she should trust government assurances that all records of the key kept outside the escrow agents have been destroyed.[380]

Two telephones communicating via Clipper Chips use the same session key; thus, when Alice and Bob are talking, a public servant with a warrant for Alice's telephone does not need to know Bob's chip key to decrypt the conversation. Knowing Alice's chip key will suffice because Alice's LEAF will provide all the information needed. Except for the fact that he is overheard talking to Alice, Bob's security is unaffected by a wiretap of Alice's line.

But if Alice and Bob are using e-mail to communicate and Capstone Chips[381] to do their encryption, both Bob and the public servant are in a different position. Capstone is designed to allow Alice and Bob to use public key encryption for their session keys.[382] Bob's Fortezza card knows Alice's public key, but not her private key or her chip key, so the only LEAF it is able to generate is one that relies on Bob's own chip key. This creates a lot of work for a public servant tapping Alice's line. Every time she gets an e-mail from a new correspondent, the public servant must decrypt its LEAF with the family key and then go to the escrow agents and request the chip unique key for the new person. If Alice communicates with many people who use Fortezza cards, the public servant may wind up holding a large, and rather valuable, collection of chip keys.

Because the wiretap order mentions only Alice, the court that issued the order has discretion to decide whether each of the people whose session keys were disclosed should be notified of that

---

There is no comparable notification duty for those wiretaps governed by the Foreign Intelligence Surveillance Act of 1978. *See* 50 U.S.C. §§ 1801-1811 (1988). The EES proposal requires no additional reporting to the subjects of such wiretaps.

[379] In practice, replacement is likely to require getting a whole new telephone because one of the aims of the EES program is to make it difficult to obtain chips to reverse engineer.

[380] Upon the expiration of the authority for a wiretap, the public servants are supposed to destroy the key information stored in the Decrypt Processor. *See* Denning & Smid, *supra* note 194, at 68.

[381] Capstone is the e-mail version of Clipper, based on the Fortezza chip. Capstone provides both encryption and digital signatures. *See supra* note 16.

[382] *See Capstone Chip Technology*, *supra* note 16.

fact.[383] Although nothing in Title III or the Attorney General's rules requires it, Bob deserves to be told.

Bob's Fortezza card will provide his digital signature as well as encryption for his e-mail. Disclosure of the digital signature key to anyone who might even be tempted to sell or make use of it would represent an enormous risk to Bob. Anyone holding Bob's key to his digital signature could masquerade as him and authenticate any transaction or correspondence (for example, in a raid on Bob's electronic bank account) with a digital signature that Bob would be powerless to disavow. Fortunately, current plans for Fortezza call for separate keys for message encryption and for digital signatures.[384] Furthermore, although Bob is powerless to change the chip unique key used to encode his e-mail's LEAF, Fortezza will allow him to change the key to his digital signature. Thus, Bob's ability to uniquely identify himself remains secure.

c. *The Status Quo May Not Be Stable*

The biggest divide between the two sides to the EES debate concerns what they consider relevant. The Clinton Administration, as one would expect, operates on the assumption that government officials can be trusted to act legally.[385] The government therefore measures the social consequences of its proposals by the effect on the government's lawful powers and the citizen's lawful rights. Critics of EES, however, tend to discount this approach. Instead, they undertake a threat analysis of the EES proposal.[386] It may seem a little silly to conduct a threat analysis of a cryptographic proposal by a government that has the raw physical power to do far worse things than spying on its citizens, but in fact threat assessment enjoys a grand tradition. The Framers of the Constitution did

---

[383] *See* 18 U.S.C. § 2518(8)(d).

[384] *See* Letter from Dorothy Denning, Professor and Chair, Computer Sciences Department, Georgetown University, to Michael Froomkin 3 (Sept. 17, 1994) (stating that the Tessera/Fortezza card stores separate keys for signatures) (on file with author).

[385] "[I]t must be presumed that federal officers will adhere to the law . . . ." Sanchez-Espinoza v. Reagan, 770 F.2d 202, 208 n.8 (D.C. Cir. 1985).

[386] Threat analysis is a long-established intelligence approach in which one assumes the worst about everyone and attempts to measure their capabilities for harm without regard to their likely or actual motives. *See, e.g.*, ANDREW COCKBURN, THE THREAT: INSIDE THE SOVIET MILITARY MACHINE 6 (1983) (describing American threat assessment of the Soviet Union's military capabilities).

not assume that "men were Angels."[387] They conducted a kind of threat analysis of government and decided that it could only be trusted if centralized power were divided in a manner that set interest against interest so as to protect the governed.[388] The impulse to rely as much as possible on structures that force proper behavior by government officials, and as little as possible on simple trust, is as old as the nation.[389]

Some of these threats to the status quo are political. For example, one glaring risk in the current EES proposal is that the escrow procedures exist entirely within the purview of the Attorney General, and could be changed at any time without any warning.[390]

Some threats consist of individual or official malefaction. In this age of spy scandals, it is always possible that the escrow agents, through negligence or corruption, may allow someone to acquire the full list of key segments.[391] The method by which keys are generated for the EES chips may lend itself to subversion of the escrow scheme from the moment the keys are generated. Although hedged with elaborate safeguards, all keys are generated by a single computer in a secure facility closed to public inspection. Because users are not in a position to monitor the key-generation procedure, they must trust that the published safeguards are being observed. Even if the risk of surreptitious subversion of the generation process were small, the risk to communications security would be greater than if the keys had never been escrowed.

---

[387] THE FEDERALIST NO. 51, at 322 (James Madison) (Clinton Rossiter ed., 1961).

[388] *See* ALBERT O. HIRSCHMAN, THE PASSIONS AND THE INTERESTS: POLITICAL ARGUMENTS FOR CAPITALISM BEFORE ITS TRIUMPH 30 (1977) (discussing *Federalist No. 51*, in which Madison justified the separation of powers as necessary to control the abuses of government).

[389] So too, of course, is the counterbalancing impulse that government is pointless if it is not effective. *See, e.g.*, McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 421 (1819) (rejecting a strict construction of the Necessary and Proper Clause in favor of a construction recognizing broad discretion in the means Congress may adopt to achieve its legitimate ends).

[390] Taking the keys out of escrow and using them might constitute a taking under the Fifth Amendment. In addition, if the government promises the public secure communications, and then attempts to go back on its promise, there may be grounds for arguing that the government violated the Due Process Clause of the Fifth Amendment by its bait and switch tactics.

[391] "Key management is the hardest part of cryptography, and often the Achilles heel of an otherwise secure system." SCHNEIER, *supra* note 12, at xvi. For examples of Cold War NSA security breaches, see KAHN, *supra* note 6, at 690-97.

Some threats to the status quo are mathematical. Critics argue that a classified algorithm such as SKIPJACK—one that has not been exposed to merciless attack by academic cryptologists—is less likely to be secure than one subject to full peer review and thus might contain an intentional, or even unintentional, "back door" that would make it vulnerable to sophisticated mathematical attack.[392] The government's response is that SKIPJACK's security is certified by the NSA[393] and by independent outside experts.[394] The government classified SKIPJACK not out of fear that publicity might expose the algorithm to attack, but to prevent users from enjoying the fruits of its research and development while at the same time avoiding participation in its key escrow system. The Administration argues that SKIPJACK is so strong that, were people able to use it without escrowing their keys, they would undermine the goal of easy government access to encrypted messages that EES is designed to achieve.[395] Some critics remain unsatisfied by this explanation. They argue that because EES is voluntary, the government should not attempt to require compliance with the escrow procedure as a condition of using SKIPJACK.[396] The Administration's response is, in effect, that if users wish to use a government-certified algorithm, they should be prepared to take the bitter with the sweet.

Some threats, perhaps the most realistic, are technological. Changes in technology are likely to make electronic eavesdropping easier, more effective, and cheaper for the government.[397] All other things being equal, a rational government would react to these changes by increasing the use of electronic eavesdropping. As government eavesdropping becomes more affordable, the reasonable citizen's desire for countermeasures ought to become greater as well.

---

[392] *See infra* note 767 and accompanying text (discussing the cryptological community's mistrust of secret algorithms).

[393] *See* Key Escrow Initiative Q&A, *supra* note 134, at 2-3.

[394] The SKIPJACK algorithm was reviewed by a panel of five distinguished outside experts who gave it their interim seal of approval. *See* SKIPJACK Interim Report, *supra* note 187, at 1, 7.

[395] *See, e.g.*, Baker Talk, *supra* note 366, at 6-10 (noting that communications protected by SKIPJACK cannot be intercepted without access to the escrow keys).

[396] *See, e.g.*, DIGITAL PRIVACY AND SECURITY WORKING GROUP, *supra* note 31, at 4.

[397] *See* Robert García, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. REV. 1043, 1053 (1991) (noting that "changes in technology are likely to increase the use of electronic eavesdropping significantly").

The technological threat appears more ominous if one tries to forecast what the government may be able to do a decade from now. Currently, all the wiretapping technology in the world is useless if there is no one to listen to the conversations. The physical and economic limit of what is currently achievable is demonstrated by the East German Ministry for State Security, the *Staatsicherheit* or Stasi, which at its peak was probably the most sophisticated and far-reaching internal surveillance organization ever created. Out of a population of 17 million, the Stasi had 34,000 officers, including 2100 agents reading mail and 6000 operatives listening to private telephone conversations, plus 150,000 active informers and up to 2 million part-time informers.[398] Together they produced dossiers on more than one out of three East Germans, amounting to one billion pages of files.[399] There are fifty-nine times more telephones in the United States than there were in East Germany and about fifteen times as many people.[400] The people (and machines) in the United States make about 3.5 trillion calls per year.[401] Even if every telephone service provider in the United States were to record every conversation in the country, the government could not make use of the tapes because it lacks the human resources necessary to listen to them. Even if political constraints could not prevent the growth of an American Stasi, the financial constraints are currently insurmountable.[402]

The cost may soon shrink dramatically. EES, the Digital Telephony initiative,[403] and advances in computer power, combined with the increasing links among federal databases[404] and

---

[398] *See* Steven Emerson, *Where Have All His Spies Gone?*, N.Y. TIMES, Aug. 12, 1990, § 6 (Magazine), at 16, 16, 19; *see also* Stephen Kinzer, *German Lawmakers Back Steps to End Spy Taint*, N.Y. TIMES, Oct. 18, 1991, at A6 (stating that the Stasi had "about 85,000 agents and several million part-time informers").

[399] *See* Emerson, *supra* note 398, at 19, 30.

[400] *See* Ferdinand Protzman, *German Overhaul Is Led by Phones*, N.Y. TIMES, Mar. 11, 1992, at D1 (reporting 1.8 million telephones in East Germany before unification—one for every 10 citizens); *see also* 1993 U.S. STATISTICAL ABSTRACT, *supra* note 38, at 563 (reporting 141.2 million telephone lines in the United States and an average of 9.773 billion telephone conversations per day).

[401] *See* 1993 U.S. STATISTICAL ABSTRACT, *supra* note 38, at 563.

[402] In 1993, the average cost of installing and monitoring a wiretap on a single subject (including those who may have had more than one telephone) was $57,256. *See* WIRETAP REPORT, *supra* note 145, at 5.

[403] *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994); *supra* note 138 and accompanying text. For a discussion of an earlier version of the Digital Telephony initiative, see Nelson, *supra* note 138.

[404] The government has already connected the databases of the Customs Service,

advances in voice recognition protocols, suggest that soon the physical constraints on widespread, government-sponsored eavesdropping may disappear. Voice recognition already allows computers to pick out a particular speaker's voice from the babble of communications;[405] combined with the power to search for particular words in all messages, this advance in technology will provide a powerful surveillance tool to any government willing to use it. Computers can monitor communications twenty-four hours per day, and they do not collect overtime. In the absence of physical and economic constraints, the only constrictions on omnipresent automated telephone monitoring will be legal and political.[406]

2. Spoofing EES: The LEAF-Blower

EES suffered a glancing blow when a researcher at AT&T discovered that it could be "spoofed," albeit with some effort.[407] The protocol that produces the spoofs quickly became popularly known as the "LEAF-blower."[408] The process is too slow to be of

---

the Drug Enforcement Agency, the IRS, the Federal Reserve, and the State Department. In addition, the Counter Narcotics Center, based at CIA headquarters, "includes agents from the FBI, the DEA, the NSA, the Defense Department, the State Department, and the Coast Guard." García, *supra* note 397, at 1065. For an alarming account of the sweeping information compiled by the Treasury Department for its Financial Crimes Enforcement Network (FinCEN) and the few legal controls applicable, see Bercu, *supra* note 90. The existence of a large, and linked, database is potentially alarming because the United States has relatively few data protection statutes along the lines of the European and Canadian models. *See* Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J 1321, 1324 (1992) (stating that from an international perspective, the American legislative response to computer processing of personal data is incomplete); *see also* OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, MAKING GOVERNMENT WORK: ELECTRONIC DELIVERY OF FEDERAL SERVICES 144 (OTA-TCT-578 1993) (warning that the "extensive use of computer matching can lead to a 'virtual' national data bank, even if computer records are not centralized in one location").

[405] *See* John Markoff, *A Spy Agency Gives Contract to Cray Computer*, N.Y. TIMES, Aug. 18, 1994, at D3 (reporting that Colombian police were able to track down drug-cartel leader Pablo Escobar Gaviria by programming U.S.-supplied computers to monitor cell-phone frequencies for his voice).

[406] *See* García, *supra* note 397, at 1056 n.39 (collecting sources that detail technological advances).

[407] *See* Blaze, *supra* note 16 (manuscript at 131) (announcing the discovery of a method enabling cryptographic communication among EES processors without the transmission of a valid LEAF).

[408] Spoofing has no effect on the security of the communication other than to block access by eavesdroppers armed with the family key and the chip unique key. *See id.* (manuscript at 138-39).

much practical value in Clipper-telephone communications, but might be applied by patient e-mail users of Capstone.[409]

Recall that an EES-compliant device will only decrypt a message that comes headed by what appears to be a valid LEAF. A "spoof" replaces the real LEAF with a simulacrum, which appears valid to the decrypting chip, and even an eavesdropper armed with the family key, but is in fact meaningless. Because the actual session key is negotiated before the LEAF is generated, the absence of the true session key in the LEAF does not affect communications so long as the LEAF passes the validity check. Because the decrypting chip checks the LEAF against a 16-bit checksum,[410] which uses the actual session key as one of its inputs, a spoof requires more than just copying a LEAF off a previous transmission. A spoof is computationally complex because the spoofer must use trial and error to generate a LEAF with a phony session key whose checksum equals that of the real session key. Each time the LEAF-blower is used, an average of 32,768 LEAFs must be tried before one works. Tests at AT&T on a prototype Capstone-based PCMCIA card showed that, on average, more than forty minutes would be needed to produce a valid-looking spoof.[411]

A LEAF-blower allows a "rogue" EES device to communicate with all other EES devices, without the recipient even knowing that the sender has spoofed the chip. Because it can take up to forty-two minutes to counterfeit the LEAF, however, the technique is likely to remain primarily of interest only to very patient people. Interestingly, NIST claims it was always aware that a LEAF-blower device could be constructed. It found the risk acceptable, however, because the technique was too slow to be of practical value.[412] Furthermore, because the chip serial number contains a field identifying the manufacturer as well as the chip, anyone who decrypts a rogue LEAF with the family key will be able to recognize a bogus chip serial number without having to consult the escrow agents.[413]

---

[409] *See id.*

[410] *See supra* note 193.

[411] *See* Blaze, *supra* note 16 (manuscript at 141). Blaze cautions that the test machine was not optimized for speed. *See id.* (manuscript at 140). On the probabilistic nature of this trial-and-error approach, see *supra* text accompanying notes 123-24.

[412] *See* National Inst. Standards & Technology, *supra* note 193, at 1.

[413] *See* Posting from David Koontz to Cypherpunks Mailing List (Aug. 25, 1994) (on file with author).

Thus, the way to feign compliance with EES remains preencrypting the message with some other system before using the EES device. Preencryption is undetectable with the family key alone, but is discernable only after the escrow agents have released the chip unique key. Preencryption is relatively easy for e-mail, but it is difficult to achieve for real-time voice communication. As a result, an eavesdropper armed with the family key should be in a good position to monitor compliance with EES even if she cannot decrypt the conversation.[414]

E. *What Happens If EES Fails?*

The large number of government orders and the attraction of SKIPJACK for those who need the security of a government-certified cryptosystem means that EES is unlikely to disappear, especially in its incarnation as the Fortezza PCMCIA card.[415] It has, however, engendered enough opposition to put its future in doubt.[416] The existence of other well-regarded ciphers such as triple-DES[417] and IDEA,[418] combined with public distaste for wiretap-ready telephones, the many unanswered questions about the proposal, the cost premium for a hardware (as opposed to a software) cryptosystem, the inflexibility of EES, and the lack of interoperability with foreign cryptosystems will likely combine to render EES if not stillborn, then at least stunted.

It seems reasonable, therefore, to speculate as to how the government will react if EES fails to become the standard. Assuming the government does not come up with a wholly new system to replace EES, two options exist:[419] (1) do nothing; or (2)

---

[414] This monitoring capability might become particularly significant in the event that the government attempts to make key escrow mandatory.

[415] *See supra* note 245 (noting large Defense Department orders of EES-compliant devices).

[416] In a poll of one thousand Americans, two-thirds found it more important to protect the privacy of phone calls than to preserve the ability of police to conduct wiretaps. When informed about the Clipper Chip, 80% said they opposed it. *See* Philip Elmer-Dewitt, *Who Should Keep the Keys?*, TIME, Mar. 14, 1994, at 90. Doubt about the Clipper has already become part of popular culture. *See, e.g.*, D.G. Chichester et al., *Tree of Knowledge: Conclusion: Softwar*, DAREDEVIL, Sept. 1994, at 1, 5 (describing Clipper Chip as a "suspicious tool"); *People Are Talking About: Big Donut*, VOGUE, Sept. 1994, at 172, 172 (asking: "How to cope?" with the Clipper Chip).

[417] *See supra* text accompanying note 131.

[418] *See infra* note 791.

[419] In either case, the government may choose to augment the hardware-based EES

forbid the use of unescrowed cryptography. The former option is implicit in the "soft sell" policy that describes EES as the price the private sector must pay for using SKIPJACK. If the private sector refuses EES, it forgoes SKIPJACK. That is its privilege, and no further government action would be needed.

The latter of the two approaches is implicit in the "hard sell" for EES. If widespread unregistered encryption can be used by "drug dealers, terrorists, and other criminals," to quote the White House,[420] then the country cannot afford to do nothing. But with unregistered cryptography already widely available, the only option may be a "Digital Volstead Act."[421]

The Clinton Administration considered banning unescrowed encryption,[422] but then concluded that it would "not propose new legislation to limit use of encryption technology."[423] A future administration might, however, reverse this decision, particularly if an investigation into a high-profile crime, such as the terrorist bombing of a major building or the management of a child pornography ring, was found to have been seriously hampered by the use of advanced cryptography. The current Administration has carefully left that option open for its successors, noting that by forgoing a ban on unescrowed encryption it is not "saying that

---

with a software key escrow standard. A software key escrow system seeks to achieve the same ends as the Clipper Chip without requiring that users purchase expensive and potentially inflexible hardware. Software-based systems are potentially more vulnerable to reverse engineering, thus increasing the danger that the cryptosystem might be converted to non-escrowed uses. Although adding software key escrow would increase the consumer appeal of escrowed encryption, there is a good chance that even this would not suffice to create a widely used standard.

[420] Office of the Press Secretary, The White House, *supra* note 292, at 1.

[421] Hoffman et al., *supra* note 26, at 112 (comparing a ban on unescrowed cryptography to the prohibition of alcohol in the 1920s).

[422] *See, e.g.*, Brock Meeks, *Cyberwire Dispatch* (Feb. 22, 1994), *available online URL* gopher://cyberwerks.com:70/00h/cyberwire/cwd/cwd.9402.22b (describing a classified April 30, 1993 memo from the Assistant Secretary of Defense stating that law enforcement and national security agencies "propose that cryptography be made available and required which contains a 'trap door' that would allow law enforcement and national security officials, under proper supervision, to decrypt enciphered communications"); John Mintz & John Schwartz, *Chipping Away at Privacy?*, WASH. POST, May 30, 1993, at H1 (describing the Administration's contingency plan to ban unescrowed encryption).

[423] LANCE J. HOFFMAN ET AL., CRYPTOGRAPHY: TRENDS IN TECHNOLOGY AND POLICY 8 (1993) (quoting Memorandum from John Podesta, Assistant to the President and Staff Secretary, The White House, to Jerry Berman, Digital Privacy and Security Working Group on Key Escrow Encryption Technology (July 29, 1993)).

'every American, as a matter of right, is entitled to an unbreakable commercial encryption product.'"[424]

The government is clearly willing to require that communications be made wiretap-ready, at least when it knows that its dictates can be enforced.[425] It is also "apparent that the law enforcement community is still looking for a way to meet its surveillance needs in the age of digital communications."[426] If EES fails, the law enforcement and intelligence communities, at least, will seek to preserve their capabilities. Legislation requiring that all strong cryptographic programs use key escrow may be the only remaining solution. As FBI Director Freeh commented, "If five years from now . . . what we are hearing is all encrypted" material that the FBI is unable to decipher, then the policy of relying on voluntary compliance with EES will have to change.[427] "The objective is for us to get those conversations whether they are . . . ones and zeros [or] wherever they are, whatever they are, I need them."[428] As a result, Part III examines the legal problems that would flow from hypothetical legislation making key escrow mandatory.

III. WOULD MANDATORY KEY ESCROW BE CONSTITUTIONAL?

A prohibition on the use of unescrowed strong cryptography for telephone or electronic mail would require federal legislation.[429] Imagine a terrorist attack on a major public building in which the conspirators protected their telephone conversations with unbreakable encryption. Aroused by such evidence of the dangers of promiscuous private encryption, Congress might well pass a law requiring that anyone using a strong cryptosystem to communicate by any electronic means acquire a license from the government. Licensed users of cryptography would either have to escrow all

---

[424] Office of the Press Secretary, The White House, *supra* note 292, at 2.

[425] *See supra* note 138 and accompanying text (discussing the Digital Telephony initiative).

[426] DIGITAL PRIVACY AND SECURITY WORKING GROUP, *supra* note 31, at 8.

[427] Louis Freeh, Keynote Luncheon Address at the International Cryptography Institute (Sept. 23, 1994) (excerpt on file with author).

[428] *Id.*

[429] *See* Memorandum from Robert D. Poling, Specialist in American Public Law, American Law Division, Congressional Research Service 2-5 (Oct. 4, 1994) (discussing current legal authority to mandate private use of the Clipper Chip, and noting that, although the Computer Security Act allows the government to set cryptographic standards for its computers, this authority applies only to the federal government's computer systems and not to civilian computer systems) (on file with author).

session keys or use a LEAF-equivalent so that the government could determine the session key without informing the parties to the communication that an investigation is in progress.

With a mandatory key escrow statute of this type, the government would be asking all citizens to surrender their collective right to technical countermeasures to the "progress of science in furnishing the Government with means of espionage."[430] Mandatory key escrow could use a hardwired chip key like Clipper, or it could be implemented through software designed to resist tampering by the user.[431] Would such a statute be constitutional?

This Part provides a whirlwind survey of relevant First, Fourth, and Fifth Amendment doctrines, as well as evolving conceptions of the constitutional right to privacy. The focus is analytic and predictive, rather than prescriptive. This Part attempts to sketch how courts, given the current state of the law, would be likely to rule on the constitutionality of a mandatory key escrow statute. It suggests that mandatory key escrow would reduce associational freedoms, chill speech, and constitute an intrusive search. The statute also might require a form of self-incrimination and would infringe personal privacy rights. Under existing doctrines, however, the analysis of the constitutionality of mandatory key escrow legislation would turn on the court's balancing of the potential costs to personal privacy against the perceived gains for law enforcement and national security. On balance, private, noncommercial users of encryption probably have a Fourth Amendment right to resist mandatory key escrow and might have a First Amendment claim as well. Whether commercial users or corporations would have such

---

[430] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[431] Trusted Information Systems has proposed a software key escrow protocol to NIST. *See* Telephone Interview with David Balenson, Senior Computer Scientist, Trusted Information Systems (June 10, 1994).

Some of the constitutional questions discussed below arguably might be avoided by focusing on standing. It might be said that because the chip (or commercial software) is produced by a corporation, and it is the corporation that is required to give the government the keys, the ultimate user thus lacks standing to complain (and, in some cases, the corporation lacks the rights enjoyed by natural persons). Because, however, much encryption occurs in software rather than hardware, and software typically generates new session keys for each communication, and these keys would not ordinarily be escrowed but for the legislation, the discussion in the text assumes that it is the end-user, whether a person or a corporation, who will have to give the government the information it seeks.

For ease of exposition, the text uses the phrase "chip key" to refer to *any* unique identifying key that allows LEAF-like access to a session key, whether the "chip key" is implemented in hardware or software.

rights under current doctrines is less clear. Even the vitality of the rights of private noncommercial users appears to be a distressingly close question given the current state of civil rights doctrine and the great importance courts accord to law enforcement and national security. A description of a more holistic, less myopic, view of the issue, as well as most recommendations, are deferred until Part IV.

The volume of relevant constitutional doctrine imposes a greater and more harmful constraint on this discussion than the need to summarize ruthlessly and put off (most) prescriptions until Part IV. Even though constitutional cases establishing a right to some form of privacy recognize that the right is grounded in the First, Fourth, and Fifth Amendments,[432] the four areas remain doctrinally distinct. Reflecting this separation for ease of exposition risks survey at the price of synergy and synthesis. It is important to remember that this is an area in which the whole is, or at least should be, greater than the sum of its clause-bound parts.

A. *First Amendment Issues*

The First Amendment states that "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble."[433] Scholars debate whether the First Amendment is a means or an end, and, if a means, then to what end.[434] Whether understood as protecting self-realization as an end in itself or political expression as a means of preserving the political process, conventional First Amendment doctrine offers numerous obstacles to mandatory key escrow. None, strangely, is insurmountable.

Mandatory key escrow affects public debate in three ways. First, mandatory key escrow forces users of cryptography to disclose

---

[432] The right to privacy also derives from the Third and Ninth Amendments. *See* Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (describing how the Third and Ninth Amendments create "zones of privacy"). This Article does not discuss the claim that the Second Amendment protects cryptography. That argument gains some force from the ITAR's classification of cryptography as a "munition," although the extent to which an administrative classification should have constitutional implications is certainly debatable. The topic would, however, require a discussion of the federal power to regulate weaponry that is beyond the scope of this Article.

[433] U.S. CONST. amend. I.

[434] *See generally* LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-1 (2d ed. 1988) (discussing whether freedom of speech is a means to some end or is an end in itself). For the view that the most important function of the First Amendment is to promote and protect democracy, see ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1972).

something they would prefer to keep secret, which amounts to compelled speech. Second, it chills speech by persons who seek to remain either secure or anonymous when speaking, whether for fear of retribution or other reasons. Third, it chills the associational freedom of persons who wish to band together but do not wish to call attention to the fact of their association or to their participation in a known association.

1. Compelled Speech

Mandatory disclosure of keys can be viewed as compelled speech, akin to laws requiring disclosure of financial records by charities and of market-sensitive information by publicly traded companies.[435] The Supreme Court treats compelled disclosure of noncommercial information as akin to a content-based restriction on speech, demanding the strictest scrutiny.[436] To pass this test, a regulation must be motivated by a compelling state interest, avoid undue burdens, and be narrowly tailored.[437] Thus, in *Wooley v. Maynard*[438] the Supreme Court struck down a New Hampshire law requiring automobiles to display license plates bearing the state motto "Live Free or Die."[439] The statute was held unconstitutional because the state required citizens to use their private property as mobile billboards for the state's message, even though the state, by allowing cars to carry disclaimers too, compelled no affirmation of belief.[440]

---

[435] Whether mandatory key escrow is compelled speech does not turn on how the government gets the keys. Although under EES the keys are provided to the government before the user buys the product, the user is still forced to send a LEAF to use the encryption. Similarly, with software encryption, users will be required to communicate the session key to the government in some fashion.

[436] *See* Riley v. National Fed'n of the Blind, 487 U.S. 781, 795 (1988) ("Mandating speech that a speaker would not otherwise make necessarily alters the content of the speech."). Thus, compelled disclosures of fact enjoy the same protection as the compelled expressions of opinion in Wooley v. Maynard, 430 U.S. 705, 713 (1977) (holding that requiring cars to display license plates bearing New Hampshire's state motto is unconstitutional), and West Virginia State Board of Education v. Barnette, 319 U.S. 624, 642 (1943) (holding that compelling individuals to recite the pledge of allegiance and salute the flag violates the First Amendment). *But see* R. George Wright, *Free Speech and the Mandated Disclosure of Information*, 25 U. RICH. L. REV. 475, 496 (1991) (arguing that a less stringent standard would have been more appropriate in *Riley*).

[437] *See Riley*, 487 U.S. at 798.

[438] 430 U.S. 705 (1977).

[439] *Id.* at 713.

[440] *See id.* at 720 (Rehnquist, J., dissenting) (stating that citizens are not "forced to affirm or reject that motto").

Mandatory key escrow differs from the issues in the leading mandatory disclosure cases[441] because the disclosure is not public. Instead, the government says it will keep the chip key secret and will decrypt the LEAF only for good cause. The Supreme Court has stated that mandatory disclosure laws will be sustained only if there is "a 'relevant correlation' or 'substantial relation' between the governmental interest and the information required to be disclosed."[442] If the state interest in telling donors how charities use their contributions is sufficient to justify a mandatory disclosure statute,[443] then the state interest in crime fighting and national security should be sufficiently compelling too.[444] Because the government keeps the key in escrow, the rule is more narrowly tailored than a public disclosure rule.[445] The critical question therefore is whether the burdens—forcing the user to utter a LEAF or the equivalent and introducing doubt as to the security of what might otherwise be a completely secure system—are worth the gain to national security and law enforcement. This is a value judgment, one that cannot be settled easily by doctrinal argument, yet one that the courts would have to make to resolve the issue.[446] As with

---

[441] In addition to *Wooley*, these include Miami Herald Publishing Co. v. Tornillo, 418 U.S. 241, 258 (1974) (holding unconstitutional a state law requiring newspapers to provide a right of reply to political candidates), and *Barnette*, 319 U.S. at 642 (finding a compulsory flag salute and recital of the pledge of allegiance unconstitutional).

[442] Buckley v. Valeo, 424 U.S. 1, 64 (1976) (citations omitted); *see also* Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 546 (1963) (holding that disclosure of membership lists requires a "substantial relation between the information sought and a . . . compelling state interest").

[443] This was the issue in Riley v. National Fed'n of the Blind, 487 U.S. 781, 781 (1988).

[444] The Supreme Court described the protection of national security as a compelling state interest in Aptheker v. Secretary of State, 378 U.S. 500, 509 (1964) ("That Congress . . . has power to safeguard our Nation's security is obvious and unarguable."). *See generally Developments in the Law—The National Security Interest and Civil Liberties*, 85 HARV. L. REV. 1130 (1972) (surveying whether national security claims justify the use of secrecy, surveillance, and emergency police powers). *But see* National Fed'n of Fed. Employees v. Greenberg, 789 F. Supp. 430, 436 (D.D.C. 1992) ("[S]ecurity concerns do not, under the American system of ordered liberty, ipso facto override all constitutional and privacy considerations. The purpose of national security is to protect American citizens, not to overwhelm their rights."), *vacated*, 983 F.2d 286 (D.C. Cir. 1993).

[445] *See* Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989) (noting that regulation is not narrowly tailored when a substantial portion of the burden on speech does not advance the state's content-neutral goals).

[446] The Supreme Court's practice of balancing constitutional rights against public needs has attracted considerable criticism. For a survey of the issues, see Symposium,

many value judgments, reasonable people may differ on the outcome; the less speculative the claim that harms will flow from allowing promiscuous unescrowed encryption (that is, the more terrorists who have managed to blow things up because they used secure telephones), the more likely the courts would find that the measure passed strict scrutiny insofar as it compels speech.[447]

2. Chilling Effect on Speech

> "Few thoughts are more threatening to people who value autonomy than the thought of being constantly watched . . . ."[448]

Because mandatory key escrow applies to all who use strong encryption, regardless of what they say, it can be considered a content-neutral regulation of speech and association.[449] As such, it is subject to an intermediate level of scrutiny involving a balancing of interests. Because mandatory key escrow directly regulates a mode of speech, the review will be more searching than it would be if the statute had only an incidental effect on speech.[450]

When Is a Line as Long as a Rock Is Heavy?: Reconciling Public Values and Individual Rights in Constitutional Adjudication, 45 HASTINGS L.J. 707 (1994).

[447] *See* TRIBE, *supra* note 434, § 12-24 (discussing the "public forum" freedom of speech doctrine).

[448] SCHEPPELE, *supra* note 1, at 302; *see also* SHOSHANA ZUBOFF, IN THE AGE OF THE SMART MACHINE: THE FUTURE OF WORK AND POWER 344-45 (1988) (describing the phenomenon of "anticipatory conformity" among persons who believe they are being observed).

[449] *See* Turner Broadcasting Sys., Inc. v. FCC, 114 S. Ct. 2445, 2459-62 (1994) (holding that a must-carry provision that distinguished between speakers solely by the technical means used to carry speech is not a content-based restriction); Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984) (allowing reasonable time, place, and manner restrictions on speech, provided such restrictions are not content-based); City Council of L.A. v. Taxpayers for Vincent, 466 U.S. 789, 804 (1984) (describing an antisign ordinance as content-neutral); Heffron v. Int'l Soc'y for Krishna Consciousness, Inc., 452 U.S. 640, 648-49 (1981) (holding a time, place, and manner regulation on all solicitations at a state fair to be content-neutral).

The act of disclosing the key might be viewed as compelled speech, in which case the compulsion would be subjected to strict scrutiny. *See supra* part III.A.1. Merely recording public information may not rise to the level of a chilling effect on speech. The Ninth Circuit rejected a Free Exercise challenge to warrantless government tape recordings of public church services at which parishioners discussed smuggling Central Americans into Arizona. *See* United States v. Aguilar, 883 F.2d 662, 694-96 (9th Cir. 1989), *cert. denied*, 498 U.S. 1046 (1991). *Aguilar* is inapposite, however, because the chip key is not public.

[450] *See generally* David S. Day, *The Incidental Regulation of Free Speech*, 42 U. MIAMI L. REV. 491 (1988) (discussing the development of the less-exacting incidental regulation doctrine for examining free speech concerns); Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46 (1987) (exploring the nature of content-neutral review); Ned Greenberg, Note, Mendelsohn v. Meese: *A First Amendment*

In practice, the Supreme Court balances the following factors: (1) the extent to which speech is likely to be chilled; (2) the degree to which the prohibition falls unevenly on a particular group as opposed to society at large; and (3) the availability of alternate channels of communication.[451] It seems evident that speech will be chilled, although exactly how much is uncertain.[452] To the extent that the prohibition falls unevenly on society, it will tend to affect those with access to computers and scrambler telephones. This is not the group whose speech the Court traditionally takes the most care to protect, because wealthy and well-educated people have the greatest access to alternative channels of communication.[453] The critical issue is likely to be whether mandatory key

---

Challenge to the Anti-Terrorism Act of 1987, 39 AM. U. L. REV. 355, 369 (1990) (distinguishing between regulations that incidentally restrict speech, which are subject to a lower level of scrutiny, and those that directly curtail speech, which are subject to a higher level of scrutiny).

[451] *See* City of Ladue v. Gilleo, 114 S. Ct. 2038, 2046 (1994) (applying the balancing test); *Clark*, 468 U.S. at 293 (same); Consolidated Edison Co. v. Public Serv. Comm'n, 447 U.S. 530, 535 (1980) (same); TRIBE, *supra* note 434, § 12-23, at 979 (stating that the Supreme Court's balancing test examines "the degree to which any given inhibition . . . falls unevenly upon various groups").

The discussion in the text assumes that a court would not find that mandatory key escrow has shut down a traditional public forum. Although mandatory key escrow most severely affects private conversation, it also affects USENET—which may be a public forum or, in universities, at least, a series of linked public fora—and other bulletin board services which may be considered private fora, *cf.* Allen S. Hammond, IV, *Regulating Broadband Communications Networks*, 9 YALE J. REG. 181, 219 (1992) (including "certain subscription technologies" within the definition of private fora), by making anonymous posting of messages less secure. If a court were to find that mandatory key escrow seriously inhibited a traditional public forum, the court would likely find the statute unconstitutional. *See* TRIBE, *supra* note 434, § 12-24, at 987 (noting that the designation "public forum" serves as "shorthand for the recognition that a particular context represents an important channel of communication in the system of free expression").

[452] On the use of computers for political speech, see Eric C. Jensen, Comment, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 FED. COMM. L.J. 217, 218-24 (1987) (noting that the growth of various types of computer bulletin boards "'brings back the era of the pamphleteer'" (quoting Lee Dembart, *The Law Versus Computers: A Confounding Terminal Case*, L.A. TIMES, Aug. 11, 1985, at D3)). Leaving aside the special case of anonymous speech, discussed below, *see infra* part III.A.3, the extent to which encrypted speech (for example, on Clipper telephones) is likely to be chilled is an empirical question on which it would be difficult to collect evidence. It is hard to measure how many people will not use encrypted telephones or e-mail if they are not confident the system is secure. It is harder still to measure how their speech changes as a result. A court considering this issue is likely to assume that the government will act legally and decrypt EES communications only when authorized. Courts are unlikely to accept that reasonable people might disagree, although whether they would, and how much, is the central empirical question.

[453] *See* TRIBE, *supra* note 434, § 12-23, at 979-80 (describing how the Court seeks

escrow "'unduly constrict[s] the opportunities for free expression.'"[454] Because a mandatory key escrow scheme promises to release keys only with just cause, the Court would likely find the constricting effect to be relatively minor. Ultimately, however, the standard collapses into a balancing test in which distinguishing "due" from "undue" content-neutral restrictions requires highly contextual judgments.[455]

3. Anonymity and the Freedom of Association

"[L]ets hold more chat.
In private then.
I am best pleased with that."[456]

Anonymity is "essential for the survival of [some] dissident movements."[457] Identification requirements "extend beyond restrictions on time and place—they chill discussion itself."[458] They also can infringe the right of assembly.[459] Cryptography allows unprec-

---

to avoid upholding communicative limits with a disproportionate impact on the poor, because the poor have the fewest alternative communication channels).

[454] *City of Ladue*, 114 S. Ct. at 2045 n.13 (1994) (quoting Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 58 (1987)); *see also* Wayte v. United States, 470 U.S. 598, 611 (1985) (noting that part of the test is whether an "incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest" (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968))).

[455] Perhaps as a result, in a recent First Amendment case no five justices were able to agree on a disposition, even though the Court unanimously agreed that the intermediate standard applied. *See* Turner Broadcasting Sys., Inc. v. FCC, 114 S. Ct. 2445, 2475 (Stevens, J., concurring in part and concurring in judgment) (voting to remand so that five justices would agree on a disposition of the appeal, despite his belief that the Court should affirm). *See generally* T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L.J. 943 (1987) (discussing the implications of Supreme Court "balancing").

[456] WILLIAM SHAKESPEARE, LOVE'S LABOUR'S LOST act 5, sc. 2, ll. 228-29 (Richard David ed., 1956).

[457] TRIBE, *supra* note 434, § 12-26, at 1019; *see also* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 91 (1982) ("The Constitution protects against the compelled disclosure of political associations and beliefs."); Gilmore v. City of Montgomery, 417 U.S. 556, 575 (1974) (noting that the right to associate freely promotes democracy); NAACP v. Button, 371 U.S. 415, 431 (1963) (refusing to permit compelled disclosure of political affiliation); Talley v. California, 362 U.S. 60, 65 (1960) (striking down a statute forbidding distribution of anonymous handbills); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) (warning that forced disclosure of affiliation with certain groups may inhibit freedom of association).

[458] Hynes v. Mayor of Oradell, 425 U.S. 610, 628 (1976) (Brennan, J., concurring in part).

[459] *See* Bates v. City of Little Rock, 361 U.S. 516, 522-24 (1960) (holding, on freedom of assembly grounds, that the NAACP did not have to disclose its

edented anonymity both to groups who communicate in complete secrecy and to individuals who, by sending electronic mail through anonymizing remailers, can hide all traces of their identity when they send mail to other persons.[460] Combined with the ability to broadcast messages widely using services such as the Internet, anonymous e-mail may become the modern equivalent of the anonymous handbill. Unlike the anonymous handbill, the anonymous remailer can allow two-way communication in which neither party can determine the identity of the other party.[461] By encrypting their return addresses using a public key belonging to the remailer, all parties can carry on a conversation without revealing their identities. If the parties use a series of secure remailers as intermediaries, and if they encrypt the text of their messages, no one will be able to connect the parties to the communication. Cryptography thus enhances communicative privacy and anonymity.

Key escrow threatens this anonymity in two ways. First, and of greater significance, it makes it possible for eavesdroppers armed with the escrowed key to identify the ultimate source and actual content of encrypted e-mail messages being sent out to anonymous remailers. Second, key escrow makes it possible for eavesdroppers armed with the escrowed key to identify the person to whom the target of a wiretap is speaking; without the key, the only information gleaned would be call set-up information, which merely identifies the telephone on the other end of the conversation.

In the last thirty years, the Supreme Court has struck down several statutes requiring public disclosure of the names of members of dissident groups,[462] stating that "[i]nviolability of privacy in

---

membership lists).

[460] *See* Timothy C. May, *The Cyphernomicon* §§ 2.9, 8.5 (Sept. 10, 1994), *available online URL* ftp://ftp.netcom.com/pub/tc/tcmay/cyphernomicon. A hypertext version of this document is available from URL: http://www.apocalypse.org/pub/nelson/bin.cgi/cypernomicon.

[461] *See id.* § 8.5.

[462] *See, e.g.*, Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations"); *Hynes*, 425 U.S. at 623 (Brennan, J., concurring in part) (asserting that a disclosure requirement puts an impermissible burden on political expression); Shelton v. Tucker, 364 U.S. 479, 485-87 (1960) (holding invalid a statute that compelled teachers to disclose associational ties because it deprived them of their right of free association); Talley v. California, 362 U.S. 60, 64-65 (1960) (voiding an ordinance that compelled the public identification of group members engaged in the dissemination of ideas); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute . . . restraint on freedom of association . . . ."));

group association may in many circumstances be indispensable to preservation of freedom of association."[463] Nevertheless, the right to privacy in one's political associations and beliefs can be overcome by a compelling state interest.[464] Thus, the Court held that associational freedoms do not trump the application of statutes forbidding discrimination in places of public accommodation. In so doing, however, the Court reiterated that "the Constitution protects against unjustified government interference with an individual's choice to enter into and maintain certain intimate or private relationships."[465] As the Court stated in *Board of Directors of Rotary International v. Rotary Club of Duarte*,[466] two key issues affecting the degree of constitutional protection to be afforded to an association are the degree of intimacy and whether the relationship is conducted "in an atmosphere of privacy" or one where the group seeks to "keep their 'windows and doors open to the whole world.'"[467] Impediments to the right to choose one's associates, including (presumably) publicity, can violate the First Amendment.[468]

Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 145 (1951) (Black, J., concurring) (expressing the fear that dominant groups might suppress unorthodox minorities if allowed to compel disclosure of associational ties). *But see* Communist Party of the United States v. Subversive Activities Control Bd., 367 U.S. 1, 85 (1961) (declining to decide whether forced disclosure of the identities of Communist Party members was an unconstitutional restraint on free association); New York *ex rel.* Bryant v. Zimmerman, 278 U.S. 63, 77 (1928) (holding that a required filing of group members' names with the state constituted a legitimate exercise of police power).

[463] *Patterson*, 357 U.S. at 462.

[464] *See Brown*, 459 U.S. at 91-92; *see also* Buckley v. Valeo, 424 U.S. 1, 143 (1976) (upholding compulsory disclosure to FEC of names of persons donating more than $10 to campaigns, and public disclosure of contributors of over $100); Griset v. Fair Political Practices Comm'n, 884 P.2d 116, 126 (Cal. 1994) (upholding state statute banning political candidates from sending anonymous mass political mailings). In McIntyre v. Ohio Elections Comm'n, 618 N.E.2d 152, 156 (Ohio 1993), *cert. granted*, 114 S. Ct. 1047 (1994), the Ohio Supreme Court let stand a state statute forbidding the circulation of anonymous leaflets pertaining to the adoption or defeat of a ballot issue.

[465] Board of Directors of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537, 544 (1987); *see also* New York State Club Ass'n v. City of New York, 487 U.S. 1, 13 (1988) (stating that freedom of expression is a powerful tool used in the exercise of First Amendment rights); Roberts v. United States Jaycees, 468 U.S. 609, 617-19 (1984) (recognizing that an individual's First Amendment rights are not secure unless those rights may be exercised in the group context as well); Moore v. City of E. Cleveland, 431 U.S. 494, 503-04 (1977) (plurality opinion) (citing examples of intimate association).

[466] 481 U.S. 537 (1987).

[467] *Id.* at 544-45, 547.

[468] *See id.* at 548 (stating that the protections of the First Amendment imply a right to associate); *see also* Citizens Against Rent Control/Coalition for Fair Hous. v. City

A requirement that group members communicate in a fashion that is accessible to lawful government wiretaps is both less and more intrusive than a requirement that groups publish their membership lists. It is less intrusive because no actual intrusion occurs until and unless a warrant is granted allowing the government to eavesdrop on communications. It is more intrusive because, once the intrusion occurs, specific facts about individuals will be disclosed in addition to the fact of membership in the group. Thus, while a national security/law enforcement justification for a narrowly tailored limit on associational privacy is likely to be at least as compelling as the state's legitimate desire to root out invidious discrimination, the countervailing interests are arguably greater also.

Groups seeking to change the social order in ways likely to be resented by police and others in positions of power will have reason to fear that state actors will find ways to access their keys. Indeed, in *Buckley v. Valeo*[469] and again in *Brown v. Socialist Workers '74 Campaign Committee*[470] the Supreme Court recognized that minor political parties may be able to show a "reasonable probability" that disclosure of membership information will subject those identified to "threats, harassment, and reprisals"—including harassment from the government.[471] Ultimately, therefore, the courts again will be left with an essentially nonlegal value judgment: whether the interests supporting mandatory key escrow are sufficiently great to justify the increased risk of harassment to political dissidents.

A challenge to mandatory key escrow as an infringement on the freedom of association would increase its chances of success if the challengers could demonstrate that mandatory key escrow closes off a channel of anonymous communication that has no true alternative.[472] Indeed, no substitute exists for the anonymous remailer: unlike anonymous leaflets, no one can see an e-mail being created, and thanks to the anonymous remailer, no one can see it being distributed, either.

---

of Berkeley, 454 U.S. 290, 299 (1981) (holding an ordinance limiting the amount of money that may be contributed to certain political organizations to be an impermissible restraint on free association).

[469] 424 U.S. 1, 74 (1976).

[470] 459 U.S. 87, 88 (1982).

[471] *Id.* at 99-101 (describing "massive" harassment of the Socialist Workers Party by the FBI).

[472] *See* City of Ladue v. Gilleo, 114 S. Ct. 2038, 2046 (1994) (holding that flyers are not a substitute for cheap and convenient signs in front of a house).

On October 12, 1994 the Supreme Court heard arguments in *McIntyre v. Ohio Elections Commission.*[473] Like *Talley*, the *McIntyre* case concerns the validity of a state statute that imposes a flat ban on distribution of anonymous political campaign leaflets. The decision in *McIntyre* may have a very significant impact on the law surveyed in this subsection.[474]

4. The Parallel to Antimask Laws

The simmering debate over antimask laws prefigures the debate over mandatory key escrow, and demonstrates how close a question mandatory key escrow could present.[475] Mandatory key escrow would make it an offense to communicate in a manner that shields the identity of the speaker from the government. Similarly, strict liability antimask statutes prohibit mask-wearing on public property, except on designated holidays such as Halloween.[476]

In states with strict liability antimask statutes, demonstrations and all travel by masked persons are illegal. Investigators of racially motivated crimes credit antimask laws for preventing those responsible from traveling in disguise. The prohibition on masked rallies also makes it easier for police to make arrests, after the fact if necessary, when demonstrations become violent.[477] Antimask

---

[473] 618 N.E.2d 152 (Ohio 1993), *cert. granted* 114 S. Ct. 1047 (1994).

[474] Similar questions arose in Griset v. Fair Political Practices Comm'n, 884 P.2d 116, 126 (Cal. 1994) (upholding the constitutionality of a state ban on anonymous political mailings).

[475] The parallel to mandatory key escrow is imperfect because antimask laws owe their existence to efforts to curb a specific group, the Ku Klux Klan, *see* Oskar E. Rey, Note, *Antimask Laws: Exploring the Outer Bounds of Protected Speech Under the First Amendment*–State v. Miller, *260 Ga. 669, 398 S.E.2d 547 (1990)*, 66 WASH. L. REV. 1139, 1145 (1991), rather than a more generalized desire to catch criminals. The existence of a specific animus aimed at one group may itself be a First Amendment violation. *See infra* note 478 (listing cases in which courts expressed disapproval of antimask laws on free speech grounds). Furthermore, most reported cases have concentrated on whether mask-wearing constitutes symbolic speech rather than on the associational freedom claims that would most likely be the centerpiece of a First Amendment challenge to any mandatory key escrow plan.

[476] *See* Wayne R. Allen, Note, *Klan, Cloth and Constitution: Anti-Mask Laws and the First Amendment*, 25 GA. L. REV. 819, 821 n.17 (1991) (citing statutes from 10 states); Rey, *supra* note 475, at 1144 n.43 (citing additional statutes). A related type of antimask statute makes it a part of the offense to intend to interfere with the civil rights of another. *See* Allen, *supra* at 821 n.16. Additionally, 18 U.S.C. § 241 makes it a felony for two or more persons to go in disguise on public highways or on the premises of another with the intent to prevent the free exercise and enjoyment of any legal right or privilege by another citizen. *See* 18 U.S.C. § 241 (1988).

[477] *See* Allen, *supra* note 476, at 828-29.

laws have been justified as a means of helping to prevent violence, but this justification has met with a mixed reception by courts and commentators.[478] The Supreme Court of Georgia accepted that the state interest in preventing crimes of violence and intimidation associated with mask-wearing was sufficiently compelling to justify an incidental infringement on First Amendment rights.[479] On this reasoning, mandatory key escrow would probably pass constitutional muster also. Not everyone agrees, however, that First Amendment guarantees can be compromised merely by reference to the history of violence associated with mask-wearers. Some courts and commentators believe that the First Amendment requires that there be specific evidence that a particular masked person or demonstration presents a threat of violence before an antimask statute can be applied without violating the Constitution.[480]

Perhaps inhibited by the irony of having to rely on *NAACP v. Alabama* ex rel. *Patterson*,[481] few Ku Klux Klan challenges to antimask laws have been predicated on the right to associational freedom of mask-wearing travellers and demonstrators. As a result, only one state supreme court and one federal court have ruled on an associational freedom challenge to an antimask law, and they disagreed.[482] The constitutionality of antimask laws remains

---

[478] *Compare* State v. Miller, 398 S.E.2d 547, 553 (Ga. 1990) (rejecting challenge to antimask statute) *and* Walpole v. State, 68 Tenn. 370, 372-73 (1878) (same) *and* Hernandez v. Commonwealth, 406 S.E.2d 398, 401 (Va. Ct. App. 1991) (same) *with* Hernandez v. Superintendent, 800 F. Supp. 1344, 1351 n.14 (E.D. Va. 1992) (noting that the statute might have been held unconstitutional if petitioner had demonstrated that unmasking himself would have restricted his ability to enjoy free speech and freedom of association) *and* Aryan v. Mackey, 462 F. Supp. 90, 91 (N.D. Tex. 1978) (granting temporary restraining order preventing enforcement of antimask law against Iranian students demonstrating against Shah) *and* Ghafari v. Municipal Court, 150 Cal. Rptr. 813, 819 (Cal. Ct. App. 1978) (holding statute prohibiting wearing masks in public overbroad and finding that state's fear that violence will result from the mere presence of anonymous persons is "unfounded"); *compare also* Allen, *supra* note 476, at 829-30 (arguing for the validity and retention of antimask laws) *with* Rey, *supra* note 475, at 1145-46 (arguing antimask laws are unconstitutional). One way to describe the cases cited above, of course, is that the KKK loses, but Iranian students win.

[479] *See Miller*, 398 S.E.2d at 551.

[480] *Compare Aryan*, 462 F. Supp. at 93-94 (requiring concrete evidence supporting the prediction that violence will occur) *with Miller*, 398 S.E.2d at 580 (accepting history of violence as sufficient evidence).

[481] 357 U.S. 449 (1958).

[482] The Supreme Court of Georgia rejected an associational freedom argument presented by the KKK in *Miller*. *See* 398 S.E. 2d at 552-53. Relying on associational freedom, Judge Higginbotham granted a temporary restraining order preventing enforcement of an antimask law against Iranian students in *Aryan*. *See* 462 F. Supp.

largely unsettled, suggesting that the First Amendment aspects of mandatory key escrow would present an equally close and disputed question.

B. *Fourth Amendment Issues*

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." It also states that "no Warrants shall issue but upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized."[483]

Americans already acquiesce to substantial invasions of privacy by government fiat, without a warrant. We disclose personal details of our lives on tax returns. We consent to having our belongings x-rayed, opened, and searched as our persons are scanned for metal (sometimes followed by a pat-down) as a condition of being allowed to board an airplane or enter some public buildings. The law says the government may paw through a citizen's garbage without a warrant,[484] and that she lacks a reasonable expectation of privacy in relation to telephone numbers dialed.[485] The police may fly over her house in a helicopter at four hundred feet[486] and use special cameras to photograph everything below.[487] The government may

---

at 92-94.

[483] U.S. CONST. amend. IV.

[484] *See* California v. Greenwood, 486 U.S. 35, 40 (1988) (holding that the Fourth Amendment does not prohibit a warrantless search and seizure of garbage left for trash collection); *see also* United States v. Scott, 975 F.2d 927, 928-30 (1st Cir. 1992) (holding that the warrantless seizure and reconstruction of 5/32-inch pieces of shredded documents in the trash did not violate the Fourth Amendment), *cert. denied*, 113 S. Ct. 1877 (1993); United States v. Comeaux, 955 F.2d 586, 589 (8th Cir.) (permitting a warrantless search of garbage within the curtilage of the home because the garbage was readily accessible to the public), *cert. denied*, 113 S. Ct. 135 (1992); United States v. Hedrick, 922 F.2d 396, 400 (7th Cir.) (same) *cert. denied*, 112 S. Ct. 147 (1991).

[485] *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding that the installation and use of a pen register by a telephone company does not constitute a search within the meaning of the Fourth Amendment). The rationale is that because people are aware that the telephone company keeps this information for billing purposes, they cannot reasonably expect that the information will be kept secret. *See id.* at 742. This is neither necessarily true, nor timelessly true, nor beyond the ability of persons and service providers to change by contract, but it is still the rule.

[486] *See* Florida v. Riley, 488 U.S. 445, 451-52 (1989) (plurality opinion) (holding valid a warrantless aerial surveillance of a greenhouse from four hundred feet); *see also* California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding valid a warrantless aerial surveillance of a yard enclosed by a 10-foot fence).

[487] *See* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that

use satellites to spy in her windows;[488] it may use heat-detection gear to monitor heat emanations from her home;[489] it may use dogs to sniff her luggage and her person.[490] Once the government has arranged for an informant to plant a beeper on a citizen, the government may use the signal to track the citizen's movements.[491] When national security is at risk, many procedural

---

warrantless aerial photography of a factory taken with a commercial camera from navigable airspace does not violate the Fourth Amendment).

[488] *See* Lisa J. Steele, Comment, *The View from on High: Satellite Remote Sensing Technology and the Fourth Amendment*, 6 HIGH TECH. L.J. 317, 327-33 (1991) (discussing warrantless searches by satellite and the applicable constitutional implications).

[489] *See* United States v. Pinson, 24 F.3d 1056, 1059 (8th Cir.) (holding that a warrantless use of infrared sensing devices did not violate the Fourth Amendment because any defendant's subjective expectation of privacy in heat emanating from her house is not one that society is prepared to recognize as objectively reasonable), *cert. denied*, 115 S. Ct. 664 (1994); United States v. Kerr, 876 F.2d 1440, 1443-44 (9th Cir. 1989) (considering the absence of heat a sign of suspiciously good insulation); United States v. Domitrovich, 852 F. Supp. 1460, 1472 (E.D. Wash. 1994) (holding that thermal imaging does not constitute a "search"); United States v. Penny-Feeney, 773 F. Supp. 220, 225-28 (D. Haw. 1991) (holding that warrants are not required for the use of an infrared sensing device from navigable air space above defendant's house, and noting that heat emanating from a house may be considered a sign that the occupants are growing marijuana within), *aff'd on other grounds sub nom.* United States v. Feeney, 984 F.2d 1053 (9th Cir. 1993); *cf.* United States v. Kyllo, 37 F.3d 526, 530 (9th Cir. 1994) (remanding for a hearing on the "intrusiveness" of thermal imaging in order to lay a factual foundation for a ruling on whether thermal imaging is a search within the meaning of the Fourth Amendment). *But see* United States v. Ishmael, 843 F. Supp. 205, 209-10, 212 (E.D. Tex. 1994) (holding that defendants had a reasonable expectation of privacy in a building and its surrounding property, and therefore thermal images that were not the product of naked eye observations amounted to an illegal, warrantless search); State v. Young, 867 P.2d 593, 601 (Wash. 1994) (holding that the use of an infrared thermal detection device to perform warrantless surveillance of the defendant's home violated the Washington state constitution's protection of defendant's private affairs and its protection against warrantless invasion of his home, as well as the Fourth Amendment of the U.S. Constitution); *cf.* Lisa J. Steele, *Waste Heat and Garbage: The Legalization of Warrantless Infrared Searches*, 29 CRIM. L. BULL. 19 (1993) (arguing that a warrant should be required for the use of infrared photography to determine activity within a dwelling).

[490] *See* United States v. Place, 462 U.S. 696, 705-07 (1983) (finding the use of "canine sniff[s]" for narcotics detection to be inoffensive to the Fourth Amendment unless the governmental interest is outweighed by the effect of the search on the individual's liberty interest). For a review of the Supreme Court cases regarding sense-enhanced searches such as dog sniffs, wiretaps, and overflights, as well as a proposed reformulation of the warrant requirement that focuses on sense-enhanced searches most susceptible to abuse, see generally David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563 (1990).

[491] United States v. Karo, 468 U.S. 705, 715-18 (1984) (noting that, although the monitoring of a beeper is not per se unconstitutional, such monitoring of a person's home is a violation of the Fourth Amendment if the individual has a justifiable interest in the privacy of the residence); *see also* United States v. Knotts, 460 U.S. 276,

protections that are required in the ordinary course of an investigation are suspended. For example, the government may, for reasons of national security, break into some premises without a warrant to plant a bug, whereas the same action in an ordinary criminal investigation would require a warrant.[492] National security wiretap requests go to a secret court that meets in camera and never issues opinions.[493]

On the other hand, mandatory key escrow differs from each of these examples in significant ways, especially as it affects private, noncommercial use. Absent exigent circumstances such as fires, hot pursuit, or the like, the Supreme Court has yet to approve a

---

282-85 (1983) (holding that police monitoring of signals does not constitute a search if the police could legitimately monitor the same activities by other legal means). *But cf.* Note, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297 (1985) (criticizing the *Knotts* and *Karo* decisions).

[492] Warrantless wiretaps are authorized by the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1802(a) (1988). The President, acting through the Attorney General, may authorize electronic surveillance for up to one year if the surveillance is directed solely at communications between or among foreign powers, there is no substantial likelihood of acquiring communication of U.S. citizens, and minimization procedures have been followed. *See id.* Title 18 of the U.S. Code also permits warrantless surveillance in emergency situations involving immediate danger, death, or serious physical injury to any persons; conspiratorial activities threatening the national interest; or conspiratorial activities characteristic of organized crime. *See* 18 U.S.C. § 2518(7) (1988).

[493] All of the court's activities are classified. It is widely believed, however, that the FISA court, as it is known, has yet to turn down a wiretap request.

The Attorney General's reports indicate that not one of the more than 4200 FISA wiretap requests was turned down during the Court's first 10 years. *See* Cinquegrana, *supra* note 196, at 814-15; *see also* ACM REPORT, *supra* note 15, at 18. The Court did turn down a request for authorization for a break-in, denying it on the dual jurisdictional grounds that the Court lacked the statutory authority to issue such an order and that the President has the inherent authority to order domestic national security surveillance without need of a court order. *See* Cinquegrana, *supra* note 196, at 823.

Congress recently authorized the FISA court to issue warrants for national security break-ins and inspections of the interior of buildings by "technical means." Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, tit. VIII, sec. 807(a), § 301(5), 108 Stat. 3423, 3444 (1994) (to be codified at 50 U.S.C. § 1821). This authority can be used against American citizens if the Justice Department persuades the FISA court that the suspects are agents of a foreign power. *See id.* § 301(b), 108 Stat. 3423, 3445; *see also* United States v. Humphrey, 629 F.2d 908, 912-14 (2d Cir. 1980) (holding that a warrantless search did not violate the Fourth Amendment because it was related to national security); *In re* Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property (F.I.S.C. 1981) (holding that a FISA order was not required, and was at any rate unavailable due to lack of jurisdiction, for a warrantless national security break-in), *reprinted in* S. REP. NO. 280, 97th Cong., 1st Sess. 16 (1981).

warrantless intrusion into a home occupied by an ordinary taxpayer, much less one who has made efforts to shield herself from detection.[494] Except for consent to x-rays and searches at airports and public buildings, none of the examples above require the target of the probe to take any action to aid the prober, much less to ensure that the probe is successful; and this exception does not reach into the home.

In principle, warrants are required for all domestic security wiretaps.[495] The next subsections describe how the Fourth Amendment also prohibits warrantless mandatory key escrow for private, noncommercial uses of encryption.[496] Commercial and corporate uses, however, present a more difficult question. These uses may not be entitled to Fourth Amendment protection against mandatory key escrow.

1. The Fourth Amendment Does Not Give the Government an Affirmative Right to an Effective Search

The government's residual prerogative under the Fourth Amendment to make reasonable searches does not empower it to require that people help to create the conditions that would make such searches effective, even if the government has valid grounds for the search. The Fourth Amendment does not create rights for the government. It creates rights for the people.[497] Congress's

---

[494] The Supreme Court *has* allowed warrantless searches of homes occupied by parolees, probationers, or welfare recipients. *See infra* text accompanying note 524. Lower courts have sanctioned two additional exceptions to this rule. First, some courts have approved warrantless national security break-ins (presumably, however, the premises were not specifically designed to resist such break-ins). Second, as described *supra* note 489, several lower courts have allowed warrantless infrared inspections of properties, including at least one property that was carefully insulated.

[495] *See* United States v. United States Dist. Court (The *Keith* Case), 407 U.S. 297, 314-21 (1972) (holding that a warrantless wiretap violated Fourth Amendment rights and implicated First Amendment policies).

[496] Fourth Amendment privacy in this context begins with the premise that people have control over who knows what about them and "the right to shape the 'self' that they present[] to the world." TRIBE, *supra* note 434, § 15-16, at 1389-90. This control is protected by the Fourth Amendment freedom from unlawful searches and seizures. *See id.*

[497] "[T]he purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government . . . ." United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990); *see also* O'Connor v. Ortega, 480 U.S. 709, 730 (1987) (Scalia, J., concurring) (stating that the Fourth Amendment serves primarily to protect the right of privacy); Warden v. Hayden, 387 U.S. 294, 303-05 (1967) (same).

power to criminalize conduct and the executive's power to enforce the criminal laws of the United States stem from the grants of power in Articles I and II of the Constitution, such as the Commerce Clause[498] and the Necessary and Proper Clause.[499] Those powers are, in turn, limited by the Bill of Rights, of which the Fourth Amendment is a part.

The absence in the Fourth Amendment of an affirmative grant of power to make effective searches, however, does not determine whether the affirmative grants in Articles I and II give the government the power to subject communications to nonconsensual searches. It simply means that from a Fourth Amendment perspective, mandatory key escrow poses strictly traditional problems: Is mandatory key escrow, which takes place without a warrant, a search and seizure?[500] If so, is it a reasonable warrantless search or seizure, or should a warrant be required?

2. Mandatory Escrow of a Key Is a Fourth Amendment "Search or Seizure"

A search is a governmental invasion of a "reasonable expectation[] of [personal] privacy."[501] Nonconsensual searches by the

---

[498] U.S. CONST. art. I, § 8, cl. 3.

[499] U.S. CONST. art. I, § 8, cl. 18. Technically, federal courts are involved solely in the adjudication of crimes that the legislative authority has defined and to which it has affixed punishments, because they cannot define common-law crimes. *See* United States v. Hudson, 11 U.S. (7 Cranch) 32, 34 (1812) (holding that the circuit courts of the United States cannot exercise common-law jurisdiction in criminal cases). Note that Article II is also involved in a different type of enforcement because some searches against agents of foreign powers operating either in the United States or abroad can be conducted pursuant to the President's national security powers. *See* 50 U.S.C. § 1802(a) (1988) (granting the President a limited power to authorize electronic surveillance for up to one year).

[500] For an argument that a mandatory key escrow scheme is a search, and thus would violate the Fourth Amendment's particularity requirement, see Mark I. Koffsky, Comment, *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, 9 HIGH TECH. L.J. 131 (1994).

[501] Oliver v. United States, 466 U.S. 170, 178 (1984); *see also* Katz v. United States, 389 U.S. 347, 361 (1967) (holding that the Fourth Amendment protects against violations of subjective expectations of privacy that society is prepared to recognize as reasonable). Items in plain view are not considered private. *See* Horton v. California, 496 U.S. 128, 133 (1990) ("If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy."); Coolidge v. New Hampshire, 403 U.S. 443, 464-66 (1971) (plurality opinion) (describing certain circumstances in which police may, without a warrant, seize evidence in "plain view"); *see also* Minnesota v. Dickerson, 113 S. Ct. 2130, 2136-37 (1993) (extending the *Horton* rationale to items in "plain touch").

government into matters for which individuals have a (subjectively and objectively) reasonable expectation of privacy ordinarily require a search warrant.[502]

Not every acquisition of information by the government from sources reasonably expected to be private is necessarily a search. For example, the Supreme Court has held that unintrusive means of piercing personal privacy, such as overflights[503] or the use of dogs to sniff for contraband,[504] are not searches for Fourth Amendment purposes. Although wiretapping is also unobtrusive, there has been no question since *Olmstead v. United States*[505] was overturned[506] that wiretapping constitutes a Fourth Amendment search or seizure.

Not every search affecting matters reasonably expected to be private requires a warrant. Examples of legitimate warrantless searches include "regulatory searches,"[507] searches incident to valid arrests,[508] searches conducted under exigent circumstances (such as the likely destruction of evidence),[509] and border search-

---

[502] *See Katz*, 389 U.S. at 357 (noting that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions" (footnotes omitted)); *cf.* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, sec. 807(a), §§ 301-309, 108 Stat. 3423, 3443-53 (1994) (to be codified at 50 U.S.C. §§ 1821-1829) (amending FISA to grant the FISA court power to issue in camera, ex parte orders authorizing physical searches and "examination of the interior of property by technical means" on a lesser showing of need than would be required for a warrant); Benjamin Wittes, *Surveillance Court Gets New Powers*, LEGAL TIMES, Nov. 7, 1994, at 1 (noting the ACLU's claim that the extension of FISA court's power is "a clear violation of the Fourth Amendment").

[503] *See* Florida v. Riley, 488 U.S. 445, 451-52 (1989) (plurality opinion) (holding that aerial police surveillance of an individual's house from a helicopter flying at four hundred feet does not offend the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 215 (1986) (finding constitutional the aerial surveillance of a yard enclosed by a 10-foot fence).

[504] *See* United States v. Place, 462 U.S. 696, 707 (1983) (holding that the use of canines in narcotics searches is not per se unconstitutional, but is subject to reasonableness requirements).

[505] 277 U.S. 438, 468-69 (1928) (holding that the admission of evidence obtained through telephone taps offends neither the Fourth nor the Fifth Amendment).

[506] *See Katz*, 389 U.S. at 353; Berger v. New York, 388 U.S. 41, 51 (1967).

[507] *See infra* text accompanying note 514.

[508] *See, e.g.*, New York v. Belton, 453 U.S. 454, 457 (1981) (stating that "a lawful custodial arrest creates a situation which justifies the contemporaneous search without a warrant of the person arrested and of the immediately surrounding area").

[509] *See, e.g.*, Cupp v. Murphy, 412 U.S. 291, 295-96 (1973) (justifying a warrantless search on the grounds that an arrestee will be "sufficiently apprised of his suspected role in the crime to motivate him to destroy what evidence he [can]"); Schmerber v. California, 384 U.S. 757, 769-71 (1966) (concluding that the rapid depletion of

es.[510] Absent a specific national security rationale directly related to the conversation, the speaker, or exigent circumstances, however, a warrant is required for a wiretap both under the Fourth Amendment and under Title III.[511]

A key is not itself a conversation, however, but the means to decrypt one. Nevertheless, there should be no doubt that absent government action to force disclosure, a properly guarded key to a cryptographic system would be an item of information for which the user would have both a subjectively and objectively reasonable expectation of privacy.[512] Indeed, the entire point of having a cryptographic system is to increase or create privacy. This is especially true in a public-key cryptographic system, in which the private key is never disclosed.[513] A requirement that keys (or the means to decrypt them) be turned over to the government is thus clearly a search or seizure for Fourth Amendment purposes.

The Fourth Amendment regulates both the issuance of search warrants and the conduct of a valid search. Key escrow seeks to preserve the government's ability to carry out a valid search by taking action in advance of any warrant.

One can imagine many actions that the government might take to preserve its ability to conduct valid searches. It might, for example, require all citizens to live in glass houses by prohibiting the use of any other building material. More reasonably, the government might prevent banks from renting out safe deposit boxes that would destroy the contents unless opened with the right key. Or, the government might prohibit the construction of homes with armored walls. Each of these hypothetical rules might raise constitutional problems, but none of them is in itself a search.

---

alcohol in the human bloodstream justifies a warrantless blood-alcohol test).

[510] *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537-38 (1985) (noting that the longstanding tradition of conducting warrantless searches of persons entering the United States reflects a concern for "the protection of the integrity of the border"); United States v. Martinez-Fuerte, 428 U.S. 543, 557 (1976) (stating that the need to make routine stops at border checkpoints in order to prevent the entrance of smugglers and illegal aliens outweighs any intrusion on Fourth Amendment interests); California Bankers Ass'n v. Schultz, 416 U.S. 21, 62-63 (1974) (dictum) (stating that those "leaving the country may be examined as to their belongings and effects, all without violating the Fourth Amendment").

[511] *See* 18 U.S.C. § 2518 (1988 & Supp. V 1993); *see also supra* notes 502-06 and accompanying text (discussing the Fourth Amendment's warrant requirement).

[512] *But see supra* note 211 and text following note 338 (describing a reason to doubt user expectations of privacy).

[513] *See infra* Technical Appendix, part B (describing a public-key cryptographic system).

In contrast, a key is information that the government forces the user to disclose. This distinguishes key escrow from other, closely related, hypothetical situations in which the government might make preemptive rules designed to make the execution of a valid search warrant easier. The dissimilarity is, however, nothing more than a weak and unreliable distinction between requiring an act and proscribing alternatives to that act. The question then becomes whether this search or seizure falls into any of the classes of exceptions to the warrant requirement.

3. Mandatory Key Escrow as a "Regulatory Search"

Only the regulatory search exception to the warrant and particularity requirements of the Fourth Amendment seems at all likely to apply to mandatory key escrow, but this single exception is enough. The requirement that all users of strong cryptography escrow their chip keys or other means to decrypt their session keys closely resembles routinized searches, such as employee drug testing, for which the Supreme Court no longer requires a warrant. Unlike traditional law enforcement searches, which are designed to find evidence of a crime, regulatory searches are "aimed at deterrence of wrongdoing through fear of detection."[514] Like the warrantless, wide-ranging, regulatory searches approved by the Supreme Court, the government's acquisition of keys will not provide evidence of anything criminal. Rather, by requiring the disclosure of keys, the government seeks to remove the shield of strong cryptography from what it believes would otherwise be socially undesirable uses.

The leading regulatory search case is *National Treasury Employees Union v. Von Raab*,[515] in which the Supreme Court endorsed a

---

[514] Craig M. Cornish & Donald B. Louria, *Employment Drug Testing, Preventive Searches, and the Future of Privacy*, 33 WM. & MARY L. REV. 95, 98 (1991).

[515] 489 U.S. 656 (1989); *see also* Florida v. Bostick, 501 U.S. 429, 434 (1991) (holding that random approaches to passengers in buses, conducted pursuant to passengers' consent, are not per se unconstitutional); Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990) (classifying suspicionless sobriety checkpoints to deter drunk driving as reasonable under the Fourth Amendment); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 634 (1989) (finding drug and alcohol tests mandated by Federal Railroad Administration regulations reasonable under the Fourth Amendment); Marshall v. Barlow's, Inc., 429 U.S. 1347, 1347 (1977) (granting stay of injunction against further warrantless searches of workplaces permitted under the Occupational Safety and Health Act of 1970, Pub L. No. 91-596, 84 Stat. 1590 (codified as amended in scattered sections of 5 U.S.C., 15 U.S.C., 18 U.S.C., 29 U.S.C., and 42 U.S.C. (1988 & Supp. V 1993))). *But see* Camara v. Municipal Court,

Customs Service program of mandatory employee drug testing.[516] The Court stated that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance."[517] Instead, "where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement," one should "balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."[518]

It is difficult to imagine a case in which the government would find it easier to plead "special needs," such as the need to prevent the development of "hidden conditions" and the impracticality of warrants for every key,[519] than in its attempt to compile a database of chip keys or session keys.[520] Mandatory key escrow fits several of the criteria enunciated in *Von Raab*. In particular, mandatory key escrow is not designed to produce evidence for criminal prosecutions (wiretaps do that, but they require warrants or other authorization), but rather to deter crimes that might otherwise be furthered by the use of encryption.[521] The key's owner knows that the key is being escrowed. In addition, if encryption becomes widespread, a more particularized approach would be difficult if not impossible.[522] Finally, because the government only plans to use the key segments for legitimate searches, it can argue that the cost to personal privacy is low.[523]

---

387 U.S. 523, 540 (1967) (finding that the defendant had a constitutional right to deny a housing inspector entry into a leasehold without a warrant in a nonemergency situation).

[516] *See Von Raab*, 489 U.S. at 665.

[517] *Id.*

[518] *Id.* at 665-66 (citing *Skinner*, 489 U.S. at 619-20).

[519] *Id.* at 668 (offering hidden conditions and impracticality as examples of "compelling" special needs) (citing *Skinner*, 489 U.S. at 624).

[520] The special needs standard has received strong criticism from academic commentators. *See* William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 554 & n.10 (1992) (summarizing criticisms).

[521] *See Von Raab*, 489 U.S. at 666 (explaining that the Customs Service's mandatory employee drug testing program was not designed to further criminal prosecutions, but to ensure that drug users did not ascend to certain positions in the service).

[522] *Cf.* United States v. Martinez-Fuerte, 428 U.S. 543, 557 (1976) (stating that requiring particularized suspicion before routine stops on major highways near the Mexican border "would be impractical because the flow of traffic tends to be too heavy to allow the particularized study of a given car that would enable it to be identified as a possible carrier of illegal aliens").

[523] "A determination of the standard of reasonableness applicable to a particular

On the other hand, although the courts have allowed warrantless regulatory searches in the workplace, at airports, in prisons, at the border, and in schools, none of the leading regulatory search cases has involved a search that entered into the home, unless the home was the scene of a fire or was occupied by a parolee, probationer, or welfare recipient.[524] Indeed, in *Camara v. Municipal Court*[525] the Supreme Court refused to eliminate the warrant requirement for routine searches that penetrated residential property hunting for violations of the city's housing code.[526] The Court characterized the housing inspectors' intrusions into the home as too "significant" to be allowed without a warrant[527]—although the same Court then went on to balance the interests at stake and concluded that warrants could be issued with a lesser showing of need than that traditionally required for probable cause.[528]

Mandatory key escrow would affect many different types of users, including both business and personal users who send messages both commercial and political. The regulatory search precedents, particularly *Von Raab*, suggest that Congress might be able to require mandatory key escrow for businesses and other commercial users without implicating the Fourth Amendment as it is currently understood. The broad sweep of the special needs justification, however, is not easily confined to the market sector of society, and there is nothing in the logic of *Von Raab* that requires it remain there.

Although the Court decided *Wyman v. James*[529] after *Camara*, to date the Court has not extended the special needs justification of *Von Raab* into the home. This suggests that private, noncommercial

---

class of searches requires 'balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.'" O'Connor v. Ortega, 480 U.S. 709, 719 (1987) (citations omitted).

[524] *See* WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 3.9 (2d ed. 1992).

[525] 387 U.S. 523 (1967).

[526] *See id.* at 534, 538-39.

[527] *See id.* at 534.

[528] *See id.* at 536-39. The *Camera* Court relied on several factors absent from the mandatory key escrow scenario for its holding, including the "long history of judicial and public acceptance" of housing code inspections. *Id.* at 537.

[529] 400 U.S. 309, 316-18 (1971) (holding that a mandatory (and warrantless) home visit by a welfare caseworker does not violate any of the welfare recipient's Fourth Amendment rights). The breadth of the special needs justification becomes particularly clear when one considers the means by which the *Wyman* Court permitted warrantless intrusions into welfare recipients' homes. *See id.*

users of encryption might not fall within any of the currently specified special needs categories of the regulatory search exception to the Fourth Amendment. As currently understood, therefore, the Fourth Amendment probably prohibits warrantless mandatory key escrow, at least for private, noncommercial users of encryption.[530]

C. *Fifth Amendment Issues*

The Fifth Amendment guarantees that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[531] The "'historic function'" of this part of the Fifth Amendment is to protect a "'natural individual from compulsory incrimination through his own testimony or personal records.'"[532] Currently, there is a tension in the Supreme Court's treatment of the reach of the Fifth Amendment. On the one hand, the Court interprets the right narrowly, to apply to criminal defendants only.[533]

> [Although the Court] has often stated [that the Fifth Amendment] protect[s] personal privacy, . . . [the] Court has never suggested that every invasion of privacy violates the privilege. . . . [T]he Court has never on any ground, personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which, in the Court's view, did not involve compelled testimonial self-incrimination of some sort.[534]

On the other hand, the Court has never questioned the special nature of some private noncommercial personal papers, such as diaries, and has held that these retain their Fifth as well as Fourth Amendment protection.[535]

With one exception, neither the Fourth nor the Fifth Amendment has ever been understood to allow the government to require

---

[530] Given the plasticity of the special needs doctrine, it is possible that the Court would extend the regulatory search exception to the home user of encryption. Extending the logic of *Von Raab* to the home, however, would gut much of what remains of the Fourth Amendment, and is a result to be avoided at all costs.

[531] U.S. CONST. amend. V.

[532] Andresen v. Maryland, 427 U.S. 463, 470-71 (1976) (holding that business records are outside the Fifth Amendment privilege) (quoting United States v. White, 322 U.S. 694, 701 (1944)).

[533] "Although conduct by law enforcement officials prior to trial may ultimately impair that right, a constitutional violation occurs only at trial." United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990) (citations omitted).

[534] Fisher v. United States, 425 U.S. 391, 399 (1976) (citations omitted).

[535] *See, e.g.*, Nixon v. Administrator of Gen. Servs., 433 U.S. 425, 459 & n.22 (1977) (noting that the most personal of documents are entitled to special protection). The protection is from subpoenas only, not search warrants.

civilians, in peacetime, to structure their lives to make hypothetical future searches by law enforcement easy. That exception, the required records doctrine, is inapposite to mandatory key escrow.[536] Instead, the Fifth Amendment is potentially relevant to mandatory key escrow in two ways. The required disclosure of the chip key resembles the required disclosure of a private paper, which may have some Fifth Amendment protection, and the forced utterance of a LEAF may be the type of incriminating testimony proscribed by the Fifth Amendment.

1. The Chip Key as a Private Paper

In *Boyd v. United States*,[537] the Supreme Court stated that private papers are an owner's "dearest property."[538] Relying on both the Fourth and Fifth Amendments, the Court found that allowing the state to compel production of that property would be "abhorrent to the instincts" of an American and "contrary to the principles of a free government."[539] As recently as *Bellis v. United States*,[540] the Supreme Court reemphasized that the Fifth Amendment protects "'a private inner sanctum of individual feeling and thought'—an inner sanctum which necessarily includes an individual's papers and effects to the extent that the privilege bars their

---

[536] The required records doctrine came into full flower in Shapiro v. United States, 335 U.S. 1, 32-33 (1948), which upheld a subpoena for incriminatory records that were required under a wartime price control statute. Later cases made clear, however, that there are limits to the government's power to define records as "required" and hence outside the protections of the Fifth Amendment. *See* Marchetti v. United States, 390 U.S. 39, 48-49 (1968) (holding that a registration requirement violated the Fifth Amendment because it materially increased the chances of prosecution); Grosso v. United States, 390 U.S. 62, 64-67 (1968) (holding that a statute requiring the reporting of, and payment of an excise tax on, earnings from wagering violated the Fifth Amendment because it was inherently self-incriminatory). Other cases have cast doubt on the firmness of these limits. *See, e.g.*, California v. Byers, 402 U.S. 424, 434 (1971) (plurality opinion) (requiring that a hit-and-run motorist identify himself). One thing beyond dispute, however, is that the government needs a court order to get access to required records. Because the point of a mandatory key escrow scheme would be to get access to the keys without a court order, the required records exception is irrelevant.

[537] 116 U.S. 616 (1886).

[538] *Id.* at 627-28.

[539] *Id.* at 632. Judge Friendly criticized this statement as "ringing but vacuous" because it "tells us almost everything, except why." Henry J. Friendly, *The Fifth Amendment Tomorrow: The Case for Constitutional Change*, 37 U. CIN. L. REV. 671, 682 (1968).

[540] 417 U.S. 85 (1974).

compulsory production and authentication."[541] Nevertheless, the rule found "abhorrent" in 1886 is now practically the law.[542]

The Supreme Court has eliminated most Fifth Amendment protections from incriminating documentary evidence sought by compulsion. First, the Supreme Court narrowed the privilege so that it applies only if the act of producing papers or records, by itself, has a self-incriminatory communicative or testimonial aspect. If the act of handing over the papers is noncommunicative—that is, if it neither reveals the existence of the document nor authenticates it—then the Fifth Amendment ordinarily does not apply.[543] Second, only natural persons can find shelter under the Fifth Amendment, and only for papers they both own and control. Thus, corporations can never claim the privilege, and neither can natural persons with regard to corporate records, even if they created and now control those records.[544] Third, once papers are handed to

---

[541] *Id.* at 91 (quoting Couch v. United States, 409 U.S. 322, 327 (1973)).

[542] *See* Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 29 (1986) (examining the new framework used by the Supreme Court in applying the Fifth Amendment privilege against self-incrimination to compulsory process for documents); Note, *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, 90 HARV. L. REV. 945, 964-85 (1977) (detailing the modern approach to the Fourth and Fifth Amendments).

[543] *See* United States v. Doe, 465 U.S. 605, 613-14 (1984) (finding that the act of producing the documents at issue would involve testimonial self-incrimination, and that requiring such production therefore violated the Fifth Amendment); Fisher v. United States, 425 U.S. 391, 398-99 (1976) (holding that requiring relinquishment of the documents at issue was not a Fifth Amendment violation because no testimonial incrimination was compelled); *see also Doe*, 465 U.S. at 618 (O'Connor, J., concurring) (contending that "the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind").

In Baltimore City Department of Social Services v. Bouknight, 493 U.S. 549, 561 (1990) (holding that a mother could not invoke her Fifth Amendment privilege against a court order to produce the child she had allegedly abused), the Supreme Court, analogizing the mother's care of the child to a required record, held that producing a child was not testimonial, and therefore the Fifth Amendment did not apply. *Id.* at 556-60. In light of this decision it is fair to ask whether the Fifth Amendment applies to anything other than oral testimony.

[544] *See, e.g.*, Braswell v. United States, 487 U.S. 99, 109-10 (1988) (holding that a custodian of corporate records may not withhold them on the grounds that such production will incriminate him in violation of the Fifth Amendment); Andresen v. Maryland, 427 U.S. 463, 472-73 (1976) (holding that a legal search of the petitioner's office resulting in the seizure of voluntarily recorded business records authenticated by a prosecution witness was not a violation of the Fifth Amendment); Bellis v. United States, 417 U.S. 85, 101 (1974) (holding that a dissolved law partnership had its own institutional identity, and its records were held in a representative capacity; therefore a grand jury subpoena for those records could not be ignored on Fifth Amendment grounds); United States v. White, 322 U.S. 694, 698-99 (1944) (holding that an officer of an unincorporated labor union could not refuse, based on Fifth Amendment

another, the legitimate expectation of privacy needed to maintain a claim under either the Fourth or Fifth Amendments disappears.[545] Fourth, records required to be kept for legal or regulatory purposes are outside the privilege.[546] Fifth, and only tangentially related to documents, the Supreme Court has held that persons can be forced to perform nontestimonial acts such as giving handwriting samples.[547] Sixth, aliens outside the sovereign territory of the United States do not ordinarily enjoy Fifth Amendment rights.[548]

The Court's narrowing interpretations notwithstanding, *Boyd* is not completely toothless. *Boyd* has a residual vitality for nonbusiness, nonfinancial, private papers and documents that are kept in the home, if only because the Supreme Court has yet to compel production of such a document.[549]

2. Is a Chip Key or a Session Key "Incriminating"?

The hornbook rule is that testimony must be incriminating when uttered in order to be entitled to protection under the Fifth Amendment. The testimony must relate to past conduct and, if it does not directly incriminate ("Yes, I did it") must at least create a "substantial" and "real" hazard of prosecution for the Fifth Amendment to apply.[550]

The Fifth Amendment does not protect testimony that might become incriminating through future conduct. In *United States v.*

---

protections, to produce the union's records); Hale v. Henkel, 201 U.S. 43, 56-58 (1906) (holding that a witness who, because of statutory immunity, cannot invoke the Fifth Amendment as to oral testimony cannot invoke it against the production of books and papers).

[545] *See* Couch v. United States, 409 U.S. 322, 335-36 (1973) (holding that petitioner had no legitimate expectation of privacy when she handed her papers over to her accountant); *Bellis*, 417 U.S. at 92-93 (same, when papers were handed to a partner in a small law firm). The attorney-client privilege is an exception to this general rule.

[546] *See supra* note 536 (discussing Shapiro v. United States, 335 U.S. 1 (1948)).

[547] *See* Gilbert v. California, 388 U.S. 263, 266-67 (1967). This rule has also been applied to voice samples, *see* United States v. Wade, 388 U.S. 218, 222-23 (1967), and blood samples, *see* Schmerber v. California, 384 U.S. 757, 767 (1966).

[548] *See* Johnson v. Eisentrager, 339 U.S. 763, 771, 782-83 (1950); *cf.* United States v. Tiede, 86 F.R.D. 227, 259 (D. Berlin 1979) (holding that friendly aliens have Fifth Amendment rights when charged with civil offenses in a U.S. court outside the territory of the United States). U.S. citizens abroad, however, do have Fifth Amendment rights. *See* Reid v. Covert, 354 U.S. 1, 5 (1957) (rejecting the idea that "when the United States acts against citizens abroad it can do so free of the Bill of Rights").

[549] *See* LAFAVE & ISRAEL, *supra* note 524, § 8.12, at 701-02.

[550] Marchetti v. United States, 390 U.S. 39, 48 (1968) (holding that requiring a frequent gambler to report illegal gambling income created a reasonable basis for fear of incrimination).

Freed,[551] the Supreme Court upheld a National Firearms Act registration requirement against a Fifth Amendment claim that the disclosed information might be used against the defendant if he committed an offense with a firearm in the future.[552]

Forced disclosure of a chip key and a session key fit uneasily into this framework. The forced disclosure of a chip key[553] before the chip has ever been used to communicate cannot be incriminating because nothing has happened yet. Thus, mandatory key escrow itself fits squarely within the *Freed* rationale. In contrast, the LEAF raises a more delicate problem. Because the LEAF precedes the actual conversation, forced utterance of a LEAF could be said to fall within the *Freed* rationale also. But this is really too facile to be credible. The encrypted session key within the LEAF is unique, and it is directly tied to the conversation that follows it. In any case, whether the LEAF is part of the conversation or not, it is an utterance that creates a "substantial" and "real" hazard of prosecution if the conversation that follows is an incriminating one, and a public servant happens to be listening.[554] On the other hand, the Supreme Court has emphasized that nontestimonial compelled disclosures are not privileged,[555] and the LEAF itself is not testimonial, save insofar as it ties a particular conversation to a particular pair of chips.

In summary, the Fifth Amendment may not protect disclosure of a chip key against mandatory key escrow, but it protects individuals against the routine warrantless *use* of that key to decrypt the LEAF and, especially, to decrypt an incriminating communication. Because the stated purpose of escrowed encryption is to allow the government to retain the abilities it currently has, and the government accepts that a warrant is required to conduct a wiretap, the Fifth Amendment imposes no significant restriction on a

---

[551] 401 U.S. 601 (1971).

[552] *See id.* at 606.

[553] Recall that for the purposes of this discussion "chip key" means either the hardwired chip's unique key in a Clipper Chip (which can lead the government to the encrypted session key buried in a LEAF) or the information needed to decrypt the equivalent information generated by a software package.

[554] *See* Hoffman v. United States, 341 U.S. 479, 486 (1951) (noting that a witness's response is incriminating if it might furnish a link in the chain of evidence needed to prosecute).

[555] *See, e.g.*, Doe v. United States, 487 U.S. 201, 208 n.6 (1988) (noting that a communication does not become privileged just because "'it will lead to incriminating evidence'" (quoting *In re* Grand Jury Subpoena, 826 F.2d 1166, 1172 n.2 (2d Cir. 1987) (concurring opinion))).

mandatory key escrow proposal of the type hypothesized.

D. *Privacy Issues*

The constitutional right to privacy derives from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, although it exceeds the sum of its parts.[556] The right to privacy has at least three components: (1) a right to be left alone; (2) a right to autonomous choice regarding intimate matters; and (3) a right to autonomous choice regarding other personal matters.[557] There is no question that mandatory key escrow would infringe on each of these component rights. The question, already partly canvassed above,[558] is whether the courts would consider the intrusions reasonably related to a sufficiently compelling state interest to justify the intrusion. As might be expected, the limitations on mandatory key escrow arising from the right to privacy conform closely to those derived from the First, Fourth, and Fifth Amendments from which the privacy right partly emanates. Privacy jurisprudence is in some turmoil, however, and it is possible that privacy will prove to be the most fertile area for legal adaptation to the new challenges posed by increasing state surveillance power and compensating private responses such as cryptography.

1. The Right to Autonomous Choice Regarding Nonintimate Matters

The right to autonomous choice regarding nonintimate personal matters is the most general component of the right to privacy. More outward-looking than the right to be left alone, but more wide-ranging than the right to autonomous choice regarding intimate matters, this component relates to those important, individual, personal decisions that are fundamental without being intimate,

---

[556] That at least was Justice Harlan's view in Griswold v. Connecticut, 381 U.S. 479, 499-500 (1965) (Harlan, J., concurring) (stating that privacy derives not from penumbras in the Bill of Rights, but from fundamental ideas of ordered liberty); *cf.* Roe v. Wade, 410 U.S. 113, 152 (1973) (relying on penumbras in the Bill of Rights).

[557] For a taxonomy of taxonomies, see TRIBE, *supra* note 434, § 15-1, and Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340. For an argument that the three strands of the right to privacy are actually inimical to each other, at least in the eyes of their advocates on the Supreme Court, see generally David M. Smolin, *The Jurisprudence of Privacy in a Splintered Supreme Court*, 75 MARQ. L. REV. 975 (1992).

[558] *See supra* parts III.A-C.

such as the choice of friends, political party, vocation, and other allegiances.[559] Disputes concerning this category, such as alleged infringements of associational freedom, tend to be adjudicated directly under the rubric of one or more amendments in the Bill of Rights rather than by appeal to privacy principles. These aspects of privacy law were canvassed above[560] and will not be repeated here.

2. The Right to Be Left Alone

The right to privacy includes a generalized "right to be let alone,"[561] which includes "the individual interest in avoiding disclosure of personal matters."[562] This strand forms the basis for many claims to a right to informational privacy.[563] Informational

---

[559] *See, e.g.*, Hampton v. Mow Sun Wong, 426 U.S. 88, 103 (1976) (holding the federal government's denial of a resident alien's right to work unconstitutional under the Fifth Amendment); Lamont v. Postmaster General, 381 U.S. 301, 305 (1965) (invalidating, under the First Amendment, a statutory requirement that persons wishing to receive "communist propaganda" identify themselves to the post office); Shelton v. Tucker, 364 U.S. 479, 490 (1960) (striking down a statute requiring teachers at state-supported schools and colleges to list every organization they had joined during the prior five years); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) (holding that the NAACP had the right to refuse to disclose its membership list on behalf of its members' rights to prevent the State from compelling them to reveal their affiliation with the group); *see also, e.g.*, John H. Ely, *Democracy and the Right to Be Different*, 56 N.Y.U. L. REV. 397, 405 (1981) (arguing that the right to be different is not constitutionally protected, but that the lack of protection is not a problem because the right generally will be invoked by those who do not need protection).

[560] *See supra* part III.D.

[561] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see also* Stanley v. Georgia, 394 U.S. 557, 564 (1969) (finding a constitutional right to "receive information and ideas, regardless of their social worth").

[562] Whalen v. Roe, 429 U.S. 589, 598-99 (1977) (acknowledging the existence of the right, but finding that it could be overcome by a narrowly-tailored program designed to serve the state's "vital interest in controlling the distribution of dangerous [prescription] drugs"); *see* Gary R. Clouse, Note, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536, 547-57 (1982) (collecting and dissecting inconsistent circuit court cases dealing with the right to withhold private information). The right to be left alone, however, is insufficiently compelling to prevent a large number of physical intrusions to bodily integrity when the police seek forensic evidence relating to a criminal investigation. *See* TRIBE, *supra* note 434, at 1331 nn.4-11 (collecting cases); *supra* note 546 (same).

[563] *See, e.g.*, Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 155 (1991) (concluding that because most theories of personhood assume personal information is a crucial part of a person's identity, there must be a recognized "right to informational privacy based on personhood" and that information is property protected by the Fifth Amendment); Clouse, *supra* note 562, at 541-47 (tracing the development of the right to informational privacy, and noting the Supreme Court's use of a balancing test to determine whether an individual's

privacy is the area in which a right to privacy most easily translates into a right to secrecy. In *Whalen v. Roe*[564] the Court allowed New York state to keep a computerized list of prescription records for dangerous drugs and to require physicians to disclose the names of patients to whom they prescribed those drugs.[565] The decision balanced the social interest in informational privacy against the state's "vital interest in controlling the distribution of dangerous drugs."[566] Finding New York's program to be narrowly tailored, and replete with security provisions designed to reduce the danger of unauthorized disclosure, the Supreme Court held that the constitutional balance tilted in favor of the statute.[567]

Mandatory key escrow appears comparable in its intrusive effects to the regulatory scheme upheld in *Whalen*, so long as the courts hold the government to its promise that keys will remain secret and will be released only pursuant to a warrant or to a very limited number of other lawful orders. Without that proviso, mandatory key escrow would verge upon unjustified data collection.[568] The warning in *Whalen* that the Court is "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files"[569] suggests, however, that informational privacy rights may grow in response to new technological threats to privacy.

3. The Right to Autonomous Choice Regarding Intimate Matters

A second component of the right to privacy is a narrow individual right to make intensely personal decisions about certain intimate associations without state interference. The Court has

---

constitutional rights have been infringed by a government-mandated disclosure of information).

[564] 429 U.S. 589 (1977).

[565] *See id.* at 593, 603-04.

[566] *Id.* at 598.

[567] *See id.* at 601-04.

[568] An extreme statute, requiring broad data collection combined with a requirement that reports be available to the public, was held unconstitutional in Thornburgh v. American College of Obstetricians and Gynecologists, 476 U.S. 747 (1986). What limits there might be to data collection and the safeguards required against disclosure were issues left open in *Whalen*: "We . . . do not[] decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions." 429 U.S. at 605-06.

[569] 429 U.S. at 605.

described certain decisions about intimate association and family- and sex-related decisions as falling within a special privacy zone for "marriage, procreation, contraception, family relationships, and child rearing and education."[570] The contours of this zone have always been fuzzy, in part because of long-standing decisions forbidding certain religious minority marriage practices[571] that would logically appear to belong within the zone of privacy described by cases such as *Griswold v. Connecticut*, *Eisenstadt v. Baird*, *Paul v. Davis*, and *Roe v. Wade*.[572] The fuzziness currently is at an all-time high because of the Court's decision in *Bowers v. Hardwick*[573] and the continuing controversy concerning the right

---

[570] Paul v. Davis, 424 U.S. 693, 713 (1976); *see also* Roberts v. United States Jaycees, 468 U.S. 609, 618-22 (1984) (describing types of "personal bonds" and relationships entitled to heightened constitutional protection); Moore v. City of E. Cleveland, 431 U.S. 494, 499 (1977) (plurality opinion) (recognizing a right to choose which relatives to live with); Roe v. Wade, 410 U.S. 113, 152 (1973) (protecting the reproductive decisions of women); Doe v. Bolton, 410 U.S. 179, 197-98 (1973) (recognizing the right to make reproductive decisions without interference from a hospital committee); Eisenstadt v. Baird, 405 U.S. 438, 452-55 (1972) (protecting the procreative decisions of unmarried opposite-sex couples); Loving v. Virginia, 388 U.S. 1, 12 (1967) (endorsing the right to engage in an interracial marriage); Griswold v. Connecticut, 381 U.S. 479, 482-86 (1965) (establishing the right of married opposite-sex couples to make procreative decisions); Poe v. Ullman, 367 U.S. 497, 551-54 (1961) (Harlan, J., dissenting) (arguing that the Constitution protects the procreative decisions of married opposite-sex partners); Skinner v. Oklahoma, 316 U.S. 535, 541 (1942) (recognizing the right not to be sterilized); Pierce v. Society of Sisters, 268 U.S. 510, 534-35 (1925) (holding that parents have the right to determine the schooling of their children); Meyer v. Nebraska, 262 U.S. 390, 399-400 (1923) (recognizing a parental right to determine what language children may learn); Kenneth L. Karst, *The Freedom of Intimate Association*, 89 YALE L.J. 624, 637-38 (1980) (arguing that divorce—the freedom of disassociation—is a fundamental privacy right).

[571] *See* Cleveland v. United States, 329 U.S. 14, 18-20 (1946) (rejecting an argument that polygamous practices should be excluded from the prohibitions of the Mann Act); Reynolds v. United States, 98 U.S. 145, 165-67 (1878) (rejecting a First Amendment challenge to a statute forbidding polygamy). Both decisions remain good law.

[572] *See supra* note 570 and accompanying text (discussing cases defining zones of privacy). In addition, many states have laws prohibiting adultery that remain on the books. These laws are not currently enforced, but there is reason to believe that if they were enforced they could survive a constitutional challenge based on privacy principles. *See* Commonwealth v. Stowell, 449 N.E.2d 357, 360 (Mass. 1983) (rejecting constitutional attack against a Massachusetts adultery statute). *But see* Martin J. Siegel, *For Better or for Worse: Adultery, Crime & the Constitution*, 30 J. FAM. L. 45, 58-86 (1991/1992) (arguing that laws criminalizing adultery are unconstitutional).

[573] 478 U.S. 1039 (1986). The Supreme Court refused to extend the vision of privacy set out in the cases above to protect the sexual choices of an unmarried same-sex couple in *Bowers* and did so in a way that casts doubt on the entire strand of privacy protection for intensely personal and intimate associations. Professor Tribe describes the decision in *Bowers* as erroneous and unprincipled and predicts that it

to abortion.[574]

As applied, this second strand of privacy jurisprudence is primarily directed at the preservation of personal autonomy,[575] and especially that autonomy relating to the sexual and reproductive practices and values of the traditional family and the "traditional unmarried couple."[576] Secrecy has a role to play here too, because sometimes secrecy is a prerequisite to the exercise of autonomy, even (or especially) within the family.[577]

Furthermore, electronic communications will increasingly become a critical part of intimate association. In a world in which the commuter marriage is increasingly common, electronic communications such as the telephone, fax, and especially e-mail (which is cheaper and less intrusive than a telephone, more private than a fax, and often instantaneous) are increasingly becoming the glue that holds marriages and other intimate relationships together.[578] The current rule, which provides much greater privacy protection to the bedroom than to the intimate, transcontinental, interspousal e-mail,[579] may soon need revision.[580] Such a revi-

---

will not be followed. *See* TRIBE, *supra* note 434, § 15-21. For a thoughtful reformulation of privacy doctrines after *Bowers*, see Rubenfeld, *supra* note 4, at 750-807.

[574] *See* Planned Parenthood v. Casey, 112 S. Ct. 2791, 2824-33 (1992) (allowing certain state restrictions on abortion); Rust v. Sullivan, 500 U.S. 173, 196 (1991) (allowing government to ban the use of federal public funds for abortions and related activities).

[575] On the psychological and moral importance of allowing individuals to make voluntary choices in matters vitally affecting them, see Bruce J. Winick, *On Autonomy: Legal and Psychological Perspectives*, 37 VILL. L. REV. 1705, 1755-68 (1992); *see also* Bercu, *supra* note 90, at 402-03 (asserting that "information privacy is essential to our development and self-fulfillment as individuals").

[576] TRIBE, *supra* note 434, § 15-21.

[577] *See, e.g.*, *Planned Parenthood*, 112 S. Ct. at 2831 (striking down a statutory provision that required spousal notification prior to abortion, but upholding the statute's informed consent and reporting requirements), *overruling* Thornburgh v. American College of Obstetricians and Gynecologists, 476 U.S. 747 (1986) (invalidating the informed consent and reporting requirements of a statute restricting abortions).

[578] E-mail also allows people to meet and exchange ideas, thus increasing their chances of forming lasting relationships. *See* Steve Lohr, *Therapy on a Virtual Couch*, N.Y. TIMES, Aug. 28, 1994, at C7 (interviewing psychiatrist and novelist Avodah Offit). Indeed, in a few cases e-mail apparently has become a *substitute* for sex, as some of Dr. Offit's patients have consulted her about their "E-mail love relationships." *Id.*

[579] *But see* Lovisi v. Slayton, 539 F.2d 349, 351-52 (4th Cir.) (en banc) (holding that a marital couple's right to bring a privacy challenge to a conviction under a Virginia sodomy statute was waived due to the presence of an invited third party), *cert. denied*, 429 U.S. 977 (1976). The majority conceded, however, that the Lovisis "would [have] remain[ed] protected in their expectation of privacy" if they had only spoken or

sion should begin by reaffirming what remains of *Boyd*, particularly as it applies to personal papers such as diaries.[581]

E. *What Next?*

On balance, as the law stands today, private, noncommercial users of encryption probably have a Fourth Amendment right to resist mandatory key escrow. Whether commercial users or corporations would have such a right under current doctrines is less clear. Even the existence of the right for private, noncommercial users appears to be a distressingly close question given the current state of civil rights doctrine and the great importance that the courts give to law enforcement and national security. The law in this area has undergone great change in the past two decades, and there is no reason to believe that the evolution has stopped.

The collapse of the distinction between home and office, fueled in part by the growth of telecommuting, will place a further strain on existing rules that attempt to distinguish between private, noncommercial activities whose classical locus is the home, and less private, more commercial activities whose traditional location was the office. If the courts further erode the remnant of the zone of privacy that still surrounds the home, the growth in freedom to work at home will have come at a high price.

IV. IDEAS ARE WEAPONS

The Bill of Rights is predicated on assumptions about technological limits that may soon be falsified. For example, the First Amendment is premised on a theory of speech that never imagined that scientific speech might become inherently dangerous.[582] Some have argued that the publication of advanced cryptographic algorithms constitutes inherently dangerous speech. Although I

---

written about their activities to third parties. *Id.* at 351.

[580] The even thornier problem of the intimate, international, interspousal e-mail is beyond the scope of this Article. The question is complex because it will turn on the citizenship of the parties, their location, and other factors.

[581] "Certain intimate personal documents—a diary is the best example—are like an extension of the individual's mind. They are a substitute for the perfect memory that humans lack. Forcing an individual to give up possession of these intimate writings may be psychologically comparable to prying words from his lips." Alito, *supra* note 542, at 39.

[582] *See* BAMFORD, *supra* note 17, at 357-63 (quoting remarks of the NSA Director Bobby Ray Inman); *supra* note 162 (collecting articles on governmental attempts to suppress academic speech with arguably harmful consequences).

think these arguments are misguided because the devices described by the speech cannot directly hurt anyone, it is certainly possible to imagine that one day someone will create a device that is easy to build, runs on house current, and is incredibly destructive. Publication of the plans for such a device might be dangerous indeed, and arguably outside the First Amendment, at least as originally conceived. In light of technical changes, "the Justices are now faced . . . with the difficult task of deciding just how high a price our constitutional commitment to open, meaningful discussion requires us to pay in terms of . . . competing concerns."[583]

The Fourth Amendment also has implicit assumptions about the limits of technology that will soon break down, if they have not already done so.[584] The Fourth Amendment was written, debated, ratified, administered, and interpreted for its first two hundred years on the basis of the assumption that there are physical limits to the government's ability to make "reasonable" searches. Although this presumption has begun to fray in the face of technical augmentation of the public servant's ability to peer into private property,[585] the basic assumption that the police cannot be everywhere at once remains unshaken.[586] This assumption may have to change, and soon. If it does, our thinking about the Fourth Amendment will need to change with it.[587]

---

[583] Vincent Blasi, *The Checking Value in First Amendment Theory*, 1977 AM. B. FOUND. RES. J. 523, 525.

[584] On a related point, consider that in colonial times, "nothing even remotely resembling modern law enforcement existed." Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 824 (1994).

[585] *See supra* notes 484-92 and accompanying text.

[586] *See supra* notes 398-402 and accompanying text.

[587] One counterargument contends that the technical change that really matters is that the world is a more dangerous place than ever imagined in 1791. The size and nature of the threat to the nation's existence, including nuclear, chemical, and bacteriological weaponry, as well as systems for their rapid and/or surreptitious delivery, means that national security interests require compromises of some rights that might never have been imagined in 1791. Although this argument is powerful, I think it mistaken for two reasons. First, it understates the degree to which the fledgling United States was at risk from military and economic assault by European powers. The new Constitution was adopted precisely because the country appeared to be falling apart under the Articles of Confederation. The Spanish, French, and British each posed substantial military and economic threats. Second, granting that modern risks include extinction where previously the greatest danger was subjugation, it would take a far more immediate danger than we currently face to make it even worth considering subjecting ourselves to a surveillance state. *See generally* OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993) (analyzing panoptic thinking by integrating several social science perspectives); Harold Edgar & Benno C. Schmidt, Jr., Curtiss-Wright *Comes Home: Executive Power*

When the Bill of Rights was adopted in 1791, speech took place between persons who saw each other eye-to-eye, or who wrote letters by hand, or printed pamphlets, books, and newspapers using hand-set type. Today those forms of communication have been supplemented, and often supplanted, by electronic communications including telephones, desktop publishing, and e-mail; additionally, letters are often typed on computers before being mailed. These new media—particularly the telephone, but increasingly e-mail—are the bases of modern social and commercial relations. They play significant roles in political and cultural organizations as well.[588] Broadcasting via radio and television (including cable television) is now the dominant mode of mass communication, having long supplanted the written word. But new forms of electronic communication such as the electronic bulletin board, the Internet USENET newsgroup, and the Internet mailing list promise to revive the importance of the written word.

Under current law, a person communicating via new media is less able to ensure her privacy than were speakers in the late eighteenth century. If Thomas Jefferson wanted to speak privately to John Adams, they could go for a walk in an open field where they could see any potential eavesdroppers from a mile away.[589] Letters could be encoded with the then-unbreakable Vigenère cipher, although this would have been a slow process and was thus rarely used.[590] In contrast, modern eavesdroppers, particularly

---

and National Security Secrecy, 21 HARV. C.R.-C.L. L. REV. 349 (1986) (discussing the enlarged role of the executive in national security matters).

[588] *See, e.g.*, Frank Odasz, *Big Sky Telegraph*, 71 WHOLE EARTH REV. 32, 32 (1991) (describing the use of the Big Sky Telegraph in linking Women's Centers in distant parts of Montana); Graeme Browning, *Zapping the Capitol*, 43 NAT'L J. 2446, 2446 (1994) (discussing the use of "the worldwide web of computer networks" to lobby Congress); John H. Fund, *We Are All Pundits Now*, WALL ST. J., Nov. 8, 1994, at A22 (reporting on the role of e-mail in the campaign to defeat Speaker of the House Tom Foley in the 1994 elections).

[589] In Hester v. United States, 265 U.S. 57, 59 (1924), the Supreme Court held that an open field was not a protected area for Fourth Amendment purposes. This does not detract from the point in the text, which refers to attitudes that long predate both Olmstead v. United States, 277 U.S. 438 (1928), and *Hester*. The open fields doctrine was restated in Oliver v. United States, 466 U.S. 170, 176-77 (1984) (finding no Fourth Amendment violation stemming from a search of a field where marijuana was growing), which appears to create a safe harbor for eavesdropping. *See* Stephen A. Saltzburg, *Another Victim of Illegal Narcotics: The Fourth Amendment (As Illustrated by the Open Fields Doctrine)*, 48 U. PITT. L. REV. 1, 25 n.105 (1986) (criticizing *Oliver* for permitting new means of surveillance that are "used to invade areas which people have traditionally believed were closed to outsiders").

[590] *See supra* note 372.

wiretappers, are invisible. Strong cryptography offers the prospect of restoring the privacy enjoyed by Jefferson and Adams to anyone with a computer or a scrambler telephone, thereby making it again possible to enjoy this privacy, albeit with a larger number of correspondents spread out over greater distances.

As the preceding sections have shown, however, it is far from obvious from the Court's recent decisions that the Constitution will be read to block a future government's attempt to dampen the privacy-enhancing effects of the cryptographic revolution. Part III argued that the constitutionality of hypothetical mandatory key escrow legislation would most often turn on a balancing test in which the Supreme Court would seek to weigh security claims against privacy interests.[591] Regardless of how the Court decides to strike the balance, it will involve a process requiring decisions not compelled by any precedent. As is often the case when the law encounters new technology, the decisional law is indeterminate or at the very least distinguishable. In order to predict where the law relating to cryptography may be going and to suggest feasible alternatives, one needs to understand the concerns that are likely to influence the balance between claims asserting security and privacy interests. The remainder of this final Part looks at how this balancing of incommensurables might work.

A. *Caught Between Archetypes*

The protections we find in the Constitution turn in part on the horror stories and heroic legends we tell ourselves; constitutional law is indeed "haunted by archetypes."[592] Examples of archetypes in constitutional law include Chief Justice Marshall, President Lincoln, the *Lochner* Court, President Nixon, and the phenomenon of McCarthyism.[593] The key escrow debates have the misfortune

---

[591] *See supra* part III.D.2.

[592] Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 13 (1991). The archetype can be seen as a special type of idealized cognitive model, usually concerning something feared or loved. *See* Steven L. Winter, *The Cognitive Dimension of the* Agon *Between Legal Power and Narrative Meaning*, 87 MICH. L. REV. 2225, 2233-34 (1989). Like other idealized cognitive models, archetypes serve as reference points used to categorize experiences.

[593] For a discussion on McCarthyism as an archetype, see Kreimer, *supra* note 592, at 14 (finding that McCarthyism "has achieved the status of a negative archetype in contemporary political discourse . . . as a term of opprobrium, of classic political impropriety"). *See generally* ROBERT A. BURT, THE CONSTITUTION IN CONFLICT (1992) (deriving archetypes implicitly from American constitutional history from the figures

to be situated at the intersection of entrenched but conflicting social/political archetypes: the totalitarian state and the conspirator.

1. Big Brother

There can be no doubt that the power of the national government has grown with every response to a national challenge, be it the Civil War, subsequent wars, the depression, or the moral, political, and practical demands of the modern welfare state. The original American constitution, the Articles of Confederation, collapsed because it was too decentralized. The replacement, our current Constitution, was bitterly opposed by a substantial minority who believed it to be an overcorrection towards centralized rule.[594] Since the adoption of the Constitution, or at least since the installation of Chief Justice Marshall, the tendency has been to ratchet power towards the center, away from states. This progression is exemplified by the evolution of the Commerce Clause. Gradually, the federal power to regulate under the Commerce Clause has come to encompass almost all economic transactions, no matter how local.[595] The evolution of the formal relationship between the central government and the individual is, however, more complex. The size and complexity of the national government's economic, legal, and regulatory powers have grown greatly, but so too (if perhaps not as quickly) have the formal legal rights of the paradigmatic citizen.[596]

Despite these developments, no sophisticated constitutional analysis is necessary to recognize that the government still lacks the authority to require that every television set sold in the United States carry with it a microphone for police to eavesdrop on

---

of Hamilton, Madison, and Lincoln).

[594] *See generally* HERBERT J. STORING, WHAT THE ANTI-FEDERALISTS WERE *FOR* (1981) (explaining the role of the Anti-Federalists and arguing that they should be counted among the Founding Fathers); HERBERT J. STORING, THE COMPLETE ANTI-FEDERALIST (1981).

[595] *See, e.g.*, Wickard v. Filburn, 317 U.S. 111, 128 (1942) (holding that Congress has the power under the Commerce Clause to regulate home-grown wheat); United States v. Darby, 312 U.S. 100, 113 (1941) (finding that Congress may regulate interstate shipment of goods under Commerce Clause power).

[596] By referring to the paradigmatic citizen, I mean to indicate that where once the free, white, usually property-owning male was the person whose political rights were the subject of rights talk, the pool of relevant rights claimants now has expanded to include all adult residents.

conversations in the home.[597] The deficiencies in this proposal would not be cured by hedging the microphone's remote controls with the most elaborate safeguards and requiring careful judicial review before activating any of the devices. The very idea is, fortunately, laughable, so much so that it is hard even to imagine any government official proposing it.[598]

Similarly, it is hard to imagine that a statute designed to ease surreptitious entry by the police, requiring every citizen to give the government a set of keys to her house, would survive even cursory judicial review.[599] These hypothetical statutes require so little analysis because they immediately evoke George Orwell's *1984*.[600] Big Brother and his thought police provide a vivid archetype of state overintrusion into private life.[601]

Vivid as the Orwellian archetype may be, it is far from all-powerful, as demonstrated by the large number of dissenting opinions vainly invoking it.[602] It may be that mandatory key

---

[597] I owe the example to Mark Eckenwiler, *Letter to the Editor: This Chip Can "Clip" Americans' Civil Liberties*, NAT'L L.J., Aug. 1, 1994, at A18.

[598] Even here, alas, a small qualification may be in order. Five years ago I would have written only slightly less emphatically that a proposal to require that every telephone switching system be modified to make government wiretapping easy would be constitutional, but of course would have no chance of passage. Now this country is committed to paying at least half a billion dollars to make that plan a reality. *See supra* notes 138, 425 and accompanying text (discussing the Digital Telephony initiative).

[599] It is disturbing to note, however, that most household locks use reproducible patterns. Armed with the serial number, a call to the manufacturer makes it easy to fabricate a duplicate. The keys to most household locks are in effect held in "escrow" by their manufacturers.

[600] GEORGE ORWELL, 1984 (1948).

[601] A similarly chilling vision is found in Bentham's concept of the Panopticon—although Bentham himself found his vision of pervasive surveillance utopian rather than dystopian. *See* MICHEL FOUCAULT, POWER/KNOWLEDGE: SELECTED INTERVIEWS & OTHER WRITINGS 1972-1977, at 146-48 (Colin Gordon ed., 1980). The Orwellian archetype also gathers some of its power from the existence of surveillance states such as North Korea, the People's Republic of China (at least in some times and regions), and the former Soviet Union. *See* DAVID B. DAVIS, THE FEAR OF CONSPIRACY 265 (1971) (noting that Americans often find it "easier to blame communist conspirators for every conflict in the world than to study the origins and complexities of civil [strife]"). Orwell's *1984* is powerful because it rings too true.

[602] *See, e.g.*, Planned Parenthood v. Casey, 112 S. Ct. 2791, 2882 (1992) (Scalia, J., dissenting) (stating that the effect of *Roe*'s sudden elimination of abortion's moral stigma from the minds of many is "nothing less than Orwellian"); Austin v. Michigan State Chamber of Commerce, 494 U.S. 652, 679 (1990) (Scalia, J., dissenting) (describing a state law that prohibits the Chamber of Commerce from advertising support for political candidates as Orwellian); County of Allegheny v. ACLU, 492 U.S. 573, 678 (1989) (Kennedy, J., concurring in the judgment in part and dissenting in

escrow will produce the same public outcry as the wiretap-ready TV set[603] or a telephone that can be turned into a bugging device even when on the hook.[604] It should. And if it does, half of this Article is an exercise in pedantic overcaution, and the fact that the state of the law produces a need for such caution is a deeply damning indictment of the Burger/Rehnquist Court's privacy jurisprudence. For if it is obvious from the *Zeitgeist* that mandatory key escrow is impossible, yet far from obvious from the relevant cases, then the cases are revealed as being significantly more state-oriented and illiberal than what "society is prepared to recognize as 'reasonable.'"[605]

Even overcaution has its place. The spirit of the times is always subject to change. As a result, we have a human court to interpret the Constitution in light of changing conditions.[606] Interpreters of the Constitution are unable to be completely insensitive to the felt necessities of the times, whether consciously or not. The decision about the constitutionality of mandatory key escrow would be no exception to this rule. The same dynamic that produced the facts of *Korematsu v. United States* and the decision itself might arise again,[607] especially if those necessities are felt strongly by officials gripped by a sense of insecurity or danger.[608] "Collectively we

---

part) (describing as Orwellian the Court's screening out of religious symbols from public displays); Florida v. Riley, 488 U.S. 445, 466 (1989) (Brennan, J., dissenting) (comparing the Court's allowance of police surveillance from aircraft to a passage from Orwell's *1984*).

[603] *See supra* note 416 (describing popular opposition to Clipper). *But see supra* note 138 (describing the Digital Telephony initiative).

[604] *See* Letter from Ron Rivest, E.S. Webster Professor of Computer Science, Massachusetts Institute of Technology, to Dorothy E. Denning, Professor and Chair, Computer Sciences Department, Georgetown University 1 (Feb. 25, 1994) (on file with author) ("There are all kinds of wonderfully stupid things one could do with modern technology that could 'help' law enforcement. But merely being of assistance to law enforcement doesn't make a proposal a good thing; many such ideas are objectionable and unacceptable because of the unreasonably large cost/benefit ratio (real or psychological cost).").

[605] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (contending that Fourth Amendment jurisprudence should accommodate contemporary standards of reasonable privacy).

[606] *See, e.g.*, William N. Eskridge, Jr., *Dynamic Statutory Interpretation*, 135 U. PA. L. REV. 1479, 1479 (1987) (noting that the Constitution, like common law, is interpreted dynamically).

[607] *See supra* note 77.

[608] There are, of course, magnificent examples of executive and judicial resistance to security paranoia. *See, e.g.*, New York Times Co. v. United States, 403 U.S. 713, 718-19 (1971) (allowing a newspaper to publish the contents of classified documents); Brandenburg v. Ohio, 395 U.S. 444, 448 (1969) (striking down Ohio's criminal

face no greater challenge than maintaining sensible perspectives on national security issues," but we sometimes fail the test.[609] One need not believe that the executive is inevitably repressive or that the judiciary is inevitably supine to recognize that both of these tendencies can be found in our nation's history, and that we therefore cannot rule out their recurrence with total confidence.

2. The Conspirator

Cryptography is the conspirator's ideal tool. This fact, more than anything else, will provide the emotional (if not the legal) justification for any attempt to control the use of unescrowed cryptography. Anxiety that people will be able to do terrible things without being detected until it is too late has been a recurring worry since the Puritans colonized North America.[610]

Given the public opposition to Clipper,[611] the government is unlikely to propose mandatory key escrow without some triggering event. In the wake of a great crime, perhaps by terrorists or drug cartels—the detection of which could plausibly have been frustrated by encryption—that which today looks clearly unconstitutional might unfortunately appear more palatable.[612] Suppose, for example,

---

syndicalism statute); Kent v. Dulles, 357 U.S. 116, 130 (1958) (holding that passports cannot be denied on the basis of past or present membership in the Communist party). It was resistance by the Department of the Army—in the executive branch—that triggered the fall of McCarthy. *See* RICHARD M. FRIED, MEN AGAINST MCCARTHY 282 (1976) (describing climatic moment of Army-McCarthy hearings).

[609] Edgar & Schmidt, *supra* note 587, at 349.

[610] In fact, the worry has deep English roots, even if these are sometimes exaggerated. *See* Francis B. Sayre, *Criminal Conspiracy*, 35 HARV. L. REV. 393, 397 (1922) (discussing the period between the reigns of Edward III and Elizabeth I, during which a number of statutes were passed to suppress combinations for various specific purposes, such as treasonable designs, breaches of the peace, raising prices, and the like); *Developments in the Law–Criminal Conspiracy*, 72 HARV. L. REV. 920, 922-23 (1959) (discussing the conspiracy indictment). The first conspiracy statutes, which defined the crime in narrow terms, were enacted around 1300 in the reign of Edward I. *See* WAYNE R. LAFAVE & AUSTIN W. SCOTT, JR., CRIMINAL LAW 525 (2d ed. 1986).

[611] *See supra* note 416 and accompanying text.

[612] In fact, wartime has often provided the impetus for U.S. government censorship of communications between the United States and foreign countries. *See, e.g.*, Exec. Order No. 8985 (Dec. 19, 1941), *reprinted in* 3 C.F.R. 1047 (1938-1943) (establishing the Office of Censorship to censor, at the "absolute discretion" of the Director, "mail, cable, radio, or other means of transmission" to or from other countries), *revoked* Exec. Order No. 9631 (Sept. 28, 1945), *reprinted in* 3 C.F.R. 435 (1943-1948) (abolishing the Office of Censorship); *see also* Matthew J. Jacobs, *Assessing the Constitutionality of Press Restrictions in the Persian Gulf War*, 44 STAN. L. REV. 675, 679-86 (1992) (outlining the history of U.S. wartime battle-zone censorship).

The World War II domestic censorship regulations required that all written

that Senator McCarthy had been able to demonstrate in 1952 that Communists were using strong encryption to protect their secrets. It is not hard to believe that some form of key escrow or an outright ban on cryptography would have been proposed, if not adopted. Big Brother may yet look more comforting than the reigning criminal archetypes.

a. *Panics Over Plotters*

The fear that two or more persons may unite in common cause to carry out an unlawful or reprehensible plot against a social community and its privileged ideals is an archetypical American concern.[613] The real or imagined conspirators have varied, being alternately foreign, domestic, or an unholy alliance of the two.[614] The fear of conspirators is not a recent phenomena dating back to the McCarthy era, but rather is rooted in the Puritan jeremiad about the dangers of succumbing to Satanic, Catholic, or nonconformist

---

messages—including those hand-carried—be passed to a censor. *See* U.S. Censorship Regulations, 32 C.F.R. § 1801.3 (1945). Letters from the United States to foreign countries or U.S. possessions were to be written "in English, if possible" but if written in another language then "the name of the language used should be written in English on the face of the envelope." *Id.* § 1801.21(b). Cables and radio traffic were permitted only in English, French, Portuguese, or Spanish without special authorization. *See id.* § 1801.48.

Letters employing codes and ciphers were specifically prohibited unless authorized. *See id.* § 1891.22. Cable transmissions could use any one of nine specified commercial codes, but private codes required a special license from the Department of Censorship. Applicants for these licenses were required to provide 15 copies of their code with the application. *See id.* § 1801.49.

Telephone calls to Mexico were permitted to be in Spanish, while French was allowed in calls to Canada. Radiotelephones could use English, Spanish, French, and Portuguese "except in the event that translators are not available at the censorship point." *Id.* § 1801.74. Anonymous international calls were prohibited. All callers had to identify themselves to the censors in advance. *See id.* § 1801.71. Callers from hotels had to be identified by the management, whereas calls from pay phones were banned. *See id.* §§ 1801.72-.73.

[613] *See* ROBERT S. LEVINE, CONSPIRACY AND ROMANCE 5 (1989) (describing various fears of conspiracy in early America); Paul Marcus, *Criminal Conspiracy Law: Time to Turn Back from an Ever Expanding, Ever More Troubling Area*, 1 WM. & MARY BILL RTS. J. 1, 3-4 (1992) (discussing the generally accepted notion that consipracy is punished because joint action is more dangerous than individual action). Webster's defines conspiracy as "[a]n agreement between two or more persons to commit a crime or accomplish a legal purpose through illegal action." WEBSTER'S II NEW RIVERSIDE UNIVERSITY DICTIONARY 302 (1983).

[614] *See* DAVIS, *supra* note 601, at xiii ("If the United States has enjoyed uncommon security from the time of independence, the Americans have also been subjected to continual alarms and warnings of imminent catastrophe.").

conspiracies. "In a nation in which every man is supposed to be on the make, there is an overriding fear of being taken in."[615] Fear of conspiracy is hardly unique to America,[616] although "Americans have been curiously obsessed with the contingency of their experiment with freedom."[617] The fear of conspiracy in America is a subject so vast that no small sketch can do it justice.

The seventeenth-century Puritan colonists of New England worried about conspiracies among Indians, Quakers, witches, and the (Catholic) French, all of whom threatened the new Israel, and in so doing also threatened to prevent the fulfillment of the millennial vision that informed those communities' founding religious vision.[618] When their relations with England soured, the colonists blamed imperialistic conspiracies they believed were aiming to destroy their liberties.[619]

In the eyes of the victors, independence only made the new nation a more attractive target to its enemies. George Washington's instantly canonical Farewell Address sounded the theme, warning of the danger posed to the American nation by secret enemies. To President Washington, it was "easy to foresee that from different causes and from different quarters much pains [would] be taken, many artifices employed, to weaken" the American commitment to its new nation. Commitment to the American experiment was precarious, vulnerable, and thus would be "the point in your political fortress against which the batteries of internal and external enemies will be most constantly and actively" directing their energies, "though often covertly and insidiously."[620] The diversity of the American people, with widely varying ancestries, differing

---

[615] *Id.* at xvi.

[616] *See* RICHARD HOFSTADTER, *The Paranoid Style in American Politics*, *in* THE PARANOID STYLE IN AMERICAN POLITICS AND OTHER ESSAYS 3, 6-7 (1965) (noting that "Americans have no monopoly on the gift for paranoid improvisation").

[617] DAVIS, *supra* note 601, at xiii.

[618] *See* LEVINE, *supra* note 613, at 6-8 (arguing that conspiratorial fears helped New England colonists to define and create communities); PERRY MILLER, THE NEW ENGLAND MIND: FROM COLONY TO PROVINCE 395 (1953).

[619] *See generally* BERNARD BAILYN, THE IDEOLOGICAL ORIGINS OF THE AMERICAN REVOLUTION 95, 144-159 (1967) (arguing that the sentiment that the American colonists were faced with a conspiracy to deprive them of their freedom had deep roots in Anglo-American political culture predating the events of the struggle with England); Gordon S. Wood, *Conspiracy and the Paranoid Style: Causality and Deceit in the Eighteenth Century*, 39 WM. & MARY Q. 411 (1982) (discussing the prevalence of conspiratorial fears in colonial America).

[620] George Washington, Farewell Address (1796), *in* A COMPILATION OF THE MESSAGES AND PAPERS OF THE PRESIDENTS 205, 207 (James D. Richardson ed., 1897).

sects and creeds, and different experiences depending on class and region, served to make the nation even more vulnerable to "faction" and conspiracy.[621]

Indeed, New England was soon gripped by a panic that the (mythical) Bavarian Illuminati, a secret, French-controlled, atheistic, antidemocratic cabal, was conspiring to undermine American liberty and religion. Despite the absence of any extant Bavarian Illuminati, many believed that the United States was in grave danger and "the vast majority of New England Federalists accepted the conspiracy charges as entirely plausible, if not completely proven."[622] The evils of the Terror in post-Revolutionary France only served to confirm the awesome power of conspirators, for only a vast conspiracy could explain the otherwise bewildering series of events.[623] The image of the Terror, and the Masonic or Jacobean conspirators behind it, was one of the themes sounded to justify the Alien and Sedition Acts.[624]

A related, if less sanguinary, imagery dominated the attack on the Second Bank of the United States, an institution that Jacksonian Democrats viewed as a secretive "hydra of corruption" designed to favor the rich against the majority of the country.[625] Here, perhaps for the first time, the conspiracy was understood to be homegrown, if dominated by "aristocratic" elements fundamentally alien in spirit to the American popular democracy desired by the Jacksonians.

In the decades before the Civil War, as the threat of foreign military invasion receded, Americans were gripped by the threat of vast shadowy conspiracies in which various groups, including

---

[621] *See* DAVIS, *supra* note 601, at 68 (pointing to anti-Catholic writers who observed that the "key to Catholic strategy" was the maxim "'[d]ivide and conquer,'" by which Catholics supposedly wished to "keep the diverse groups and interests of society from fusing into 'a bona fide American character'"); Washington, *supra* note 620, at 207 (warning of the dangers of factions).

[622] PETER AMAZEEN, THE BAVARIAN ILLUMINATI SCARE 3 (1988) (unpublished B.A. thesis, Harvard University); *see also* VERNON STAUFFER, NEW ENGLAND AND THE BAVARIAN ILLUMINATI 229-43 (1918) (noting that the panic, which lasted almost two years, was touched off by a sermon given by Reverend Jedeidiah Morse on May 9, 1798, based on his reading of John Robison's 1797 book, *Proofs of a Conspiracy Against All the Religions and Governments of Europe*).

[623] *See* DAVIS, *supra* note 601, at 35.

[624] *See id.* at 36. For a discussion of the Alien and Sedition Acts, see *supra* note 75 and accompanying text.

[625] BRAY HAMMOND, BANKS AND POLITICS IN AMERICA FROM THE REVOLUTION TO THE CIVIL WAR 379 (1957) (quoting President Jackson); *see also id.* at 395-96, 405-09 (describing the various evils of the Bank as perceived by Jacksonians).

Freemasons, Mormons, or Catholics, plotted secretly to subvert the American (Protestant) way of life.[626] The American commitment to openness meant that any organization that was not itself open, that held secret meetings or, worse, had secret rituals, was not just suspect, but threatening.[627] The Civil War itself came to be portrayed as an apocalyptic battle between the forces of freedom and a conspiratorial "Slave Power."[628]

Post-Civil War industrialization provided the environment for a redefinition and bifurcation of the nature of the conspiracy, one which persisted until the First World War. On the one hand, there was the conspiracy of labor organizations, be it the International Workers of the World, the Socialist International, or the beginning of the American union movement. An illustrative example was the reaction to the Haymarket Riot of 1886, in which Chicago workers battled police, and which culminated in the explosion of a dynamite bomb that was widely ascribed to anarchists. Convictions were returned by a jury made up of persons who admitted prejudice against the defendants, and whom the judge charged to convict if "there was a conspiracy to overthrow the existing order of society" and that the defendants and the bomb-thrower, whoever he might be, were parties to it.[629] Others, notably the Progressives, focused on what they perceived was the conspiracy among corporations, trusts and a small cabal built on wealth and privilege[630] designed, they thought, to wrest control of the economy and thus undermine the democratic process.[631] The entry of the United States into the

---

[626] *See* David B. Davis, *Some Themes of Countersubversion: An Analysis of Anti-Masonic, Anti-Catholic, and Anti-Mormon Literature*, 47 MISS. VALLEY HIST. REV. 205 (1960), *reprinted in* DAVIS, *supra* note 601, at 9, 10-11. Fear of Freemasons gave rise to a major political party, the anti-Masonic party.

[627] *See id.* at 14 (citing Richard Rush for the idea that "[o]f all governments . . . ours was the one with the most to fear from secret societies, since popular sovereignty by its very nature required perfect freedom of public inquiry and judgment").

[628] *See* DAVID B. DAVIS, THE SLAVE POWER CONSPIRACY AND THE PARANOID STYLE 62-86 (1969) (describing various formulations of the "Slave Power" thesis).

[629] JACOB EPSTEIN, THE GREAT CONSPIRACY TRIAL 5-7 (1970).

[630] *See* DAVIS, *supra* note 601, at 153.

[631] *See, e.g.*, Robert M. La Follette, *A Small Group of Men Hold in Their Hands the Business of This Country*, 42 CONG. REC. 3434-36, 3450-51 (1908), *reprinted in* DAVIS, *supra* note 601, at 200. Consider too this lawyer's view of the danger:

> We have heard much of the dangers of corporations in late years; but, while our publicists had hardly whetted their swords to meet this question, we are confronted with a new monster a thousand times more terrible. Every student knows how corporations have grown from a monastic institution to the predominance they now occupy in the business world; but American ingenuity has invented a legal machine which may swallow a hundred

First World War shortly after President Wilson's promise to stay out of it, combined with Communism's triumph in Russia, unleashed an orgy of antisubversive activity, although the distinction from simple nativism was not always clear.[632]

Late-twentieth-century anti-Communist antisubversion is a topic all of its own, spanning McCarthyism,[633] loyalty oaths,[634] and a large number of important civil liberties decisions, notably those alternately expanding and contracting the protections of the First Amendment.[635] The low water mark, achieved in *Dennis v. United States*,[636] amounted to the criminalization of "any radical political doctrine."[637] Recently, in a climate of lessened insecurity, the courts have been considerably more willing to allow a wide range of radical speech.[638] The important points for present purposes are

---

> corporations or a hundred thousand individuals; and then, with all the corporate irresponsibility, their united power be stored, like a dynamo, in portable compass, and wielded by one or two men. Not even amenable to the restraints of corporation law, these "trusts" may realize the Satanic ambition,– infinite and irresponsible power free of check or conscience.

F.J. Stimson, *Trusts*, 1 HARV. L. REV. 132, 132 (1887-1888).

[632] *See* DAVIS, *supra* note 601, at 205-10 ("The years from 1917 to 1921 are probably unmatched in American history for popular hysteria, xenophobia, and paranoid suspicion."). At its peak in 1924, the Ku Klux Klan, which blended nativisism with its anti-Black, -Catholic, and -Jewish ideology, had about 4.5 million members. *See id.* at 215.

[633] *See generally* DAVID M. OSHINSKY, A CONSPIRACY SO IMMENSE: THE WORLD OF JOE MCCARTHY (1983) (tracing Senator McCarthy's life and political career).

[634] *See generally* HARRY KALVEN, JR., A WORTHY TRADITION: FREEDOM OF SPEECH IN AMERICA 340-67 (1988) (discussing Supreme Court decisions regarding loyalty oaths).

[635] *See, e.g.*, Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam) (reformulating the test first outlined in Schenck v. United States, 249 U.S. 47, 51 (1919), to require objectively inciting language in a context that makes it likely to produce direct lawless behavior in order to regulate speech); Dennis v. United States, 341 U.S. 494, 516-17 (1951) (upholding a conviction under the Smith Act for the mere advocacy of Communism); Schenck v. United States, 249 U.S. 47, 51 (1919) (creating the "clear and present danger" test for any attempted regulation of speech). *See generally* THOMAS I. EMERSON, TOWARD A GENERAL THEORY OF THE FIRST AMENDMENT (1963) (tracing the Supreme Court's development of jurisprudence protecting freedom of expression); Note, *Conspiracy and the First Amendment*, 79 YALE L.J. 872 (1970) (discussing the conflict between conspiracy law and First Amendment rights).

[636] 341 U.S. 494, 516-17 (1951) (upholding petitioner's conviction under the Smith Act despite the absence of evidence of any overt act other than the advocacy of Communism); *cf.* 3 RONALD D. ROTUNDA ET AL., TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE § 20.14, at 56 (1986) (attributing *Dennis* to the Supreme Court's bowing to the "tone of the times . . . as it managed to avoid direct confrontation" with Congress and the Executive).

[637] MARTIN M. SHAPIRO, FREEDOM OF SPEECH: THE SUPREME COURT AND JUDICIAL REVIEW 65 (1966).

[638] *See, e.g.*, Hess v. Indiana, 414 U.S. 105, 109 (1973) (per curiam) (emphasizing

that, although one could debate what constitutes the norm, decisions significantly curtailing civil liberties are far from unique and that these decisions are often driven by a fear of criminal or subversive plotters, a fear with deep roots in our culture. Given an appropriate trigger, it is entirely possible that a similar dynamic could apply to the regulation of cryptography.

b. *Modern Incarnations: The Drug Kingpin and the Terrorist*

Today's most significant criminal archetypes are the drug kingpin and the terrorist. Perhaps because criminal, anarchist, and terrorist archetypes arise from events rather than literature, there is no single figure or movement with the evocative power of Big Brother, now that the international communist conspiracy has left the anxiety closet and joined the Wobblies and the Jacobins in the care of the History Department. Jack the Ripper, the prototypical serial killer, may be the closest thing to a threatening criminal archetype that has lasted more than two generations, although Al Capone, Charles Manson, and the urban gang member all have achieved some near-mythic status as well.

What criminal archetypes lack in longevity, they make up in menace. At least until his capture, the terrorist archetype for many years was Carlos the Jackal.[639] Carlos's capture, coming as it does on the heels of the collapse of any credible international communist movement, may create a small window of opportunity for privacy activists to seek legislative or judicial ratification for their argument that Big Brother is a greater menace. This window may not be open for long.[640]

---

the requirement that speech must be "intended to produce, and likely to produce, *imminent* disorder" to be punished by the state); *Brandenburg*, 396 U.S. at 447 (reformulating *Schenck* to require objectively inciting language in a context that makes it likely to produce direct lawless behavior in order to regulate speech). *See generally* LEE C. BOLLINGER, THE TOLERANT SOCIETY: FREEDOM OF SPEECH AND EXTREMIST SPEECH IN AMERICA (1986) (arguing that over the past few decades freedom of speech has developed a new significance that helps to account for the extremes to which the principle has been taken).

[639] *See* DAVID YALLOP, TRACKING THE JACKAL: THE SEARCH FOR CARLOS, THE WORLD'S MOST WANTED MAN (1993); *see also* CLAIRE STERLING, THE TERROR NETWORK 129-46 (1981) (tracing the career of Carlos the Jackal).

[640] "Big Brother is dead. The only serious likelihood of his resurrection lies in reaction to the chaos and disintegration" that might be caused by "[t]errorists with secure phones . . . [who] could bring down not just a few buildings but large sections of a modern economy." Nicholas Wade, *Method and Madness: Little Brother*, N.Y. TIMES, Sept. 4, 1994, § 6 (Magazine), at 23.

The "War on Drugs" proclaimed by President Ronald Reagan in 1982 and enthusiastically endorsed by Presidents Bush and Clinton may be our "longest war."[641] "Refusing to shoulder" the "unbearable burden" of communities "devastated" by drugs, "Americans have given the government a mandate to eliminate the scourge before its effects become irrevocable."[642] Champions of the War on Drugs claim "almost universal acceptance [of the notion] that the drug problem is 'the worst disease that plagues our nation today.'"[643] Notably, "[b]y the mid 1980s . . . anti-drug sentiment encompassing even casual use became a national cause."[644]

Likewise, fear of the drug kingpin quickly reached Congress, which reacted first by passing the continuing criminal enterprise statute, better known as the drug kingpin statute, imposing long mandatory minimum sentences.[645] When that was not enough, Congress passed a statute permitting the death penalty in drug cases connected to a killing.[646] Along the way, Congress made attempting to be a drug kingpin and conspiring with a drug kingpin punishable by the same penalty as the offense itself.[647]

With Congress and the Executive in such agreement, it is no surprise that the War on Drugs is a major social phenomenon, having criminalized behavior engaged in by somewhere between fourteen and twenty-three million Americans per year.[648] Experts

---

[641] STEVEN B. DUKE & ALBERT C. GROSS, AMERICA'S LONGEST WAR: RETHINKING OUR TRAGIC CRUSADE AGAINST DRUGS at xv (1993).

[642] Diane-Michele Krasnow, *To Stop the Scourge: The Supreme Court's Approach to the War on Drugs*, 19 AM. J. CRIM. L. 219, 224 (1992) (discussing Supreme Court cases dealing with the "War on Drugs" in relation to the Fourth, Sixth, and Eighth Amendments).

[643] Sandra R. Acosta, *Imposing the Death Penalty upon Drug Kingpins*, 27 HARV. J. ON LEGIS. 596, 596 (1990) (quoting Representative James A. Traficant, a Democrat from Ohio).

[644] Krasnow, *supra* note 642, at 221 n.3.

[645] *See* Pub. L. No. 91-513, tit. II, § 408, 84 Stat. 1236, 1265 (1970) (codified as amended at 21 U.S.C. § 848 (1988 & Supp. V 1993)). A person engages in a continuing criminal enterprise if she "occupies a position of organizer, a supervisory position, or any other position of management" of five or more persons who act feloniously, in concert, to violate drug laws. 21 U.S.C. § 848(c)(2)(A) (1988).

[646] *See* Pub. L. No. 100-690, tit. VII, § 7001, 102 Stat. 4181, 4387 (1988) (codified as amended at 21 U.S.C. § 848 (1988 & Supp. V 1993)) (making the death penalty applicable to convictions for killings committed during illicit drug-related activity).

[647] *See* Pub. L. No. 91-513, tit. II, § 406, 84 Stat. 1236, 1265 (1970) (codified as amended at 21 U.S.C. § 846 (1988)).

[648] *See* Michael Isikoff, *Federal Study Shocks Drug Experts: "Casual" Use of Pot, Cocaine Plummets, but Coke Addiction Rises*, SACRAMENTO BEE, Aug. 1, 1989, at A1, A12 (noting that casual use of marijuana and cocaine fell from 23 million people in 1985 to 14.5 million in 1988); *see also* Randy E. Barnett, *Bad Trip: Drug Prohibition and the*

recently began to study the war's longer-term effects, including the incarceration of hundreds of thousands of persons, clogged courts, corrupt police officers and corrupt judges, and a disproportionate impact on African-American males (and, through them, on their families).[649] The War on Drugs has achieved these and other dubious results through the expedient of demonizing the drug user, the drug "pusher," and especially the drug "kingpin."[650]

The fear of drug trafficking puts great pressure on the police. The mutually consensual nature of the drug crime requires a special type of police work because "law enforcement lacks its staunchest ally, the victim,"[651] who might report the crime and testify against the perpetrator. As a result, the police are driven to use surveillance, wiretapping, and informants because they have little else upon which to rely.[652] In 1993, about two-thirds of the court-ordered wiretaps were for drug-related offenses.[653] A similar dynamic has stimulated the expansion of surveillance into the workplace.[654]

The attempt to control drug trafficking also puts pressures on the courts that go beyond increasing caseloads. The War on Drugs creates pressure to support efforts to eradicate the drug "plague." The results of such pressure include Supreme Court descriptions of drug traffickers as "sophisticated criminal syndicates" that create

---

Weakness of Public Policy, 103 YALE L.J. 2593, 2613 n.65 (1994) (book review of DUKE & GROSS, *supra* note 641).

[649] *See* DUKE & GROSS, *supra* note 641, at 160-61 (discussing the social costs of drug prohibition); Barnett, *supra* note 648, at 2610-14 (same).

[650] *See* Barnett, *supra* note 648, at 2613 (noting that demonization is made easier by the relatively small number of drug users).

[651] DUKE & GROSS, *supra* note 641, at 107.

[652] *Cf.* Barnett, *supra* note 648, at 2612 (describing the view of some commentators that police are given so much deference in searching and arresting drug suspects that there is a de facto "drug exception" to the Bill of Rights).

[653] *See* WIRETAP REPORT, *supra* note 145, at 4.

[654] *See* Cornish & Louria, *supra* note 514, at 95 (discussing the effects that mass drug testing will have on our culture by examining employment drug testing as a means of surveillance). The authors report that mass drug testing entails:

> (1) Fourth Amendment tolerance of systematic preventive searches; (2) increased use of biochemical surveillance as a means of monitoring and deterring undesired behavior; (3) increased use of the workplace and economic sanctions as a tool of regulating undesirable behavior; (4) privatization of traditional law enforcement functions; (5) shrinkage of our expectations of personal privacy; (6) increased use of "profiles"; (7) erosion of the presumption of innocence; and (8) erosion of dignity and autonomy.

Id. at 96.

an unprecedented obstacle for law enforcement.[655] In addition, the antidrug crusade has had a major impact on the Fourth Amendment: since President Reagan declared the War on Drugs, the government has prevailed in nearly every search and seizure case before the Supreme Court.[656]

As James Boyd White points out in his analysis of Chief Justice Taft's majority opinion in *Olmstead v. United States*,[657] the "organization, scale, enterprise, and success" of a criminal enterprise can become the occasion for a morality tale in which the government represents good struggling against the forces of evil.[658] In the context of actions that can be painted as enormous threats, constitutional texts like the Fourth Amendment can be made to seem irrelevant.[659] The implication for mandatory key escrow is obvious: the more closely the purposes of a statute are aligned with control of drugs or terrorism, and especially the more closely the facts of a test case conform to the apprehension of an archetypical evildoer, the less chance it will be declared unconstitutional.[660]

B. *Mediating the Clash: A Metaphoric Menu*

Social and political archetypes influence constitutional decisionmaking, but the decisions themselves are couched in more traditionally legal terms. These terms have a power of their own, which accounts for some of the law's partial autonomy as a discipline. Thus, for example, the homeless defendant in *Connecticut v. Mooney*[661] sought to exclude evidence seized from his habitual abode on public land under a bridge abutment on the ground that

---

[655] United States v. Place, 462 U.S. 696, 704 n.5 (1983).

[656] *See* Krasnow, *supra* note 642, at 240; *see also* Silas J. Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257, 264 (1984) (arguing that the Court has not only weakened the warrant and probable cause requirements, but has also avoided them by expanding Terry v. Ohio, 392 U.S. 1 (1968), and contracting the definition of a search); Steven Wisotsky, *Crackdown: The Emerging "Drug Exception" to the Bill of Rights*, 38 HASTINGS L.J. 889, 907 (1987) (noting that "[i]n recent years . . . the courts have almost always upheld the government" in search and seizure cases).

[657] 277 U.S. 438 (1928).

[658] James B. White, *Judicial Criticism*, 20 GA. L. REV. 835, 854 (1986).

[659] *See id.* (arguing that Taft's opinion is drafted to evoke a "sense that the fourth amendment has nothing to do with what is really going on in the case").

[660] Another possible trigger might be the use of cryptography to hide a child pornography ring. For an example of the likely reaction, see generally John C. Scheller, Note, *PC Peep Show: Computers, Privacy, and Child Pornography*, 27 J. MARSHALL L. REV. 989 (1994).

[661] 588 A.2d 145 (Conn.), *cert. denied*, 112 S. Ct. 330 (1991).

the place had become his "home."[662] "Home" is a powerful metaphor; it is also a legal category that implies certain outcomes and forecloses others.

It is old news that common-law legal reasoning is both analogical and taxonomical,[663] and that metaphor is a powerful tool for both.[664] Nevertheless, the observation that "[t]he power of a metaphor is that it colors and controls our subsequent thinking about its subject"[665] is particularly relevant and powerful when the law encounters a new technology.[666] The law's first reaction to a

---

[662] *See id.* at 152. The Court did not decide whether the abutment was the defendant's home for Fourth Amendment purposes. *See id.* at 155. *Compare* Teryl S. Eisenberg, Note, Connecticut v. Mooney: *Can a Homeless Person Find Privacy Under a Bridge?*, 13 PACE L. REV. 229 (1993) (arguing that a homeless person may be afforded an expectation of privacy in the area the individual reasonably considers "home" based on societal understandings of the privacy associated with a "home") *with* David H. Steinberg, Note, *Constructing Homes for the Homeless? Searching for a Fourth Amendment Standard*, 41 DUKE L.J. 1508 (1992) (arguing that the reasonable-expectation-of-privacy inquiry is based on property interests, and concluding that a homeless defendant could not have a reasonable expectation of privacy in belongings left beneath a public bridge abutment).

[663] *See, e.g.*, EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING 1-3 (1948) (outlining the case method of legal reasoning); K.N. LLEWELLYN, THE BRAMBLE BUSH 70 (1951) ("There was a view, and I suppose some hold it still, that law is made up of principles and rules. A master craftsman would be able to arrange them in one great hierarchical scheme.").

[664] *See, e.g.*, D. Marvin Jones, *Darkness Made Visible: Law, Metaphor, and the Racial Self*, 82 GEO. L.J. 437, 447-87 (1993) (applying an analysis of social and legal uses of metaphor to illuminate social construction and significance of race); Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 40 STAN. L. REV. 1371, 1382-94 (1988) (describing cognitive and legal functions of metaphor).

[665] Winter, *supra* note 664, at 1383; *see also* Donald A. Schön, *Generative Metaphor: A Perspective on Problem-Setting in Social Policy*, *in* METAPHOR AND THOUGHT 137, 137 (Andrew Ortony ed., 2d ed. 1993) (discussing the use of "metaphor" as both a kind of product and a kind of process by which "new perspectives on the world come into existence").

[666] Others have made this point before in the context of computers. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 996-1015 (1994) (distinguishing between problems such as defamation, for which existing legal categories work, and problems such as reasonableness of behavior in cyberspace, for which existing legal categories do not offer clear-cut solutions); David R. Johnson & Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 VILL. L. REV. 487, 489-90 (1993) (arguing for a contract regime in cyberspace); Henry H. Perritt, Jr., *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*, HARV. J.L. & TECH., Spring 1992, at 65, 95-113 (arguing that the common law of defamation should inform courts' treatment of tort claims arising out of communications on electronic networks); Henry H. Perritt, Jr., *Metaphors and Network Law* (Oct. 15, 1992), *available online URL* gopher://ming.law.vill.edu:70/00/.chron/.papers/.files/Metaphors.and.Network.Law.txt (arguing that print shop, broadcasting, and telephone

new technology is to reach for analogies and to explain why the new technology can be treated identically to an earlier technology. Railroads, for example, could be slotted into the existing legal categories created to deal with highways, collisions, and freight tariffs.[667] In contrast, airplanes—a technological advance on the same order as the railroad—required a significant change in the law because to be useful the airplane must fly over land, a classical trespass, without a right of way.[668]

In the case of cryptography, as with other new technologies, the dominant mode of judicial and perhaps political judgment is likely to be classification by analogy and argument by metaphor. Given that in recent years Big Brother seems to have inspired less fear in any branch of government than has Big Drugs, the selection of the right metaphor is critical.

Four metaphors seem particularly likely to appeal to the courts, which can be summarized under the rubrics of "car," "language," "house," and "safe." These four metaphors reflect two fundamentally different characterizations of cryptography. Both "car" and "language" characterize cryptography as part of the means used to transmit the message. In this view, an encrypted message is simply another communication, one which can best be understood as a special case of the general rules regulating communications. In contrast, "house" and "safe" treat cryptography as something that happens before the message leaves the sender. Both "house" and "safe" suggest that the proper approach is to start with the sender's decision to encipher the message in order to exclude unwanted recipients, and then explore the implications of this choice for the government's ability to monitor communications. The differences

---

metaphors are inadequate, and proposing alternatives based on a tort system).

[667] John Perry Barlow suggests that the development of the railroads provides a better metaphor for the growth of the Internet than does the information superhighway, because in both cases large private industries sought government-imposed standards and regulations that served to give early entrants commanding market positions. *See* John P. Barlow, *Stopping the Information Railroad, available online URL* http://www.ora.com/gnn/bus/ora/features/barlow/index.html.

[668] *See* Hinman v. Pacific Air Transp. Corp., 84 F.2d 755, 759 (9th Cir. 1936), *cert. denied*, 300 U.S. 654 (1937) (giving airplanes right of way over private property); Vincent M. Brannigan, *Biotechnology: A First Order Technico-Legal Revolution*, 16 HOFSTRA L. REV. 545, 549 (1988) (noting that some new technologies, like railroads, did not require an adjustment in legal conceptions, whereas others, like the airplane, required fundamental adjustments); Brannigan & Dayhoff, *supra* note 52, at 27 (noting that the advent of air travel "required fundamental shifts in the nature of the right to property").

among these metaphors go beyond putting a positive or negative gloss on encryption; they amount to different definitions of the nature of the thing itself. Interestingly, both the general metaphor of communication and the metaphors of exclusion are sufficiently indeterminate to permit the introduction of more specific, and contradictory, metaphors that support both sides in the mandatory EES debate.

1. Focus on Communication

"Communication" as we tend to understand it is itself a metaphor. English speakers tend to speak as if they share a particular mental image of how words work. As Michael Reddy has persuasively demonstrated, the English language defaults to a metaphor of communication as a conduit for human thoughts and feelings.[669] In this cognitive shorthand, the speaker begins with a meaning that she "puts into words," which are then "gotten across" to the auditor who then "unpacks," "gets," or "absorbs" the speaker's meaning.[670] To put it another way, the speaker/author "encodes" meanings into words that "convey" meanings that are then "decoded" by the recipient.[671]

The ubiquity of the conduit metaphor suggests that encryption, if understood as a communications conduit, stands the best chance of being accepted by the courts, Congress, and the public. The same ubiquity, however, also means that different analogic embodiments of the same general metaphor can lead to diametrically opposite views of the constitutionality of a hypothetical ban on unescrowed cryptography. Indeed, if the encrypted message is seen

---

[669] *See* Michael J. Reddy, *The Conduit Metaphor: A Case of Frame Conflict in Our Language About Language*, *in* METAPHOR AND THOUGHT, *supra* note 665, at 164, 165.

[670] *See id.* at 189-201 (giving hundreds of examples).

[671] Reddy argues that the conduit metaphor is dysfunctional because it obscures a reality in which the auditor/recipient of the communication must actively construct a new text with meaning in light of the recipient's own referents. *See id.* at 184-87; *see also* ROLAND BARTHES, THE PLEASURE OF THE TEXT 3-67 (Richard Miller trans., 1975) [hereinafter BARTHES, PLEASURE] (posing questions about and offering commentary on a reader's finding pleasure in the text she reads); ROLAND BARTHES, S/Z at 4 (Richard Miller trans., 1974) [hereinafter BARTHES, S/Z] ("Our literature is characterized by the pitiless divorce . . . between the producer of the text and its user, [which leaves the reader] with no more than the poor freedom either to accept or reject the text . . . ."). *See generally* DAVID HOLDCROFT, SAUSSURE: SIGNS, SYSTEM, AND ARBITRARINESS (1991) (discussing signs as a semantic system). The validity of this critique is not at issue here; what matters for present purposes is the accuracy of the claim that the conduit metaphor is pervasive.

as a mobile message unit—a "car" on the information superhighway—then mandatory EES appears far less troubling than if the encrypted messages are analogized to language itself.

a. *"Car"–How Messages Travel*

One could say that the escrowing of a key is akin to having one's picture taken when applying for a license to drive on the information superhighway. Or, perhaps, the chip's unique key could be seen as something like a license plate. If the reigning metaphor for use of electronic communications is that of a car on the road, it is but a small step to fixed or random checkpoints, and other minor electronic detentions.

The LEAF feature in Clipper and Capstone makes checkpoints for compliance with mandatory key escrow particularly easy to implement, in a way that other forms of escrowed encryption might not. Telephone and e-mail messages can be intercepted and copied at random, or according to some pattern, then decrypted with the family key. If there is no LEAF at all, the message is clearly in violation of the mandatory escrow rule. If there is a LEAF, although the text of the message remains inaccessible without recourse to the escrow agents,[672] public servants can check whether the message has been encrypted with an EES-compliant device because the chip serial number is supposed to contain a recognizable string identifying the manufacturer.[673] If this string is instead random, law enforcement knows it has encountered a spoofed LEAF.[674] The beauty of this system from a constitutional perspective is that the intrusion on privacy rights is relatively small. Law enforcement does not need to decrypt actual messages without a search warrant.

The car metaphor also provides law enforcement with a solution to a timing problem. The information highway patrol may not want to wait to obtain a warrant to find out whether a message's cryptography is registered. Just as police who stop cars on the highway have authority to conduct a search without a warrant,[675]

---

[672] Because the message remains unreadable, there is no way to tell whether it was preencrypted with unescrowed cryptography.

[673] *See supra* text preceding note 413.

[674] This check does not detect preencryption of e-mail. *See supra* text following note 413.

[675] *See* Chambers v. Maroney, 399 U.S. 42, 52 (1970) (applying the exigency exception to the warrant requirement to an automobile); Carroll v. United States, 267 U.S. 132, 153 (1925) (allowing an exception to the Fourth Amendment's warrant requirement in the case of movable vessels).

the same might be done on the information highway, and for similar reasons. Waiting for a warrant takes too long—the car is gone; the message is gone.[676]

The car metaphor leads naturally, at least from the law enforcement perspective, to random traffic stops. If the analogy is to vehicular checkpoints, the examination of the LEAF can easily be characterized as a minimally intrusive investigation in a way that it cannot be if the focus is on the act of encryption as something occurring in the home or office. In the case of real cars, the Supreme Court applies a reasonableness analysis to vehicle stops, weighing the gravity of the public concern, the degree to which the seizure advances that concern, and the interference with the individual's liberty. In *United States v. Martinez-Fuerte*,[677] the Court held that limited seizures of vehicles for questioning of the occupants could be constitutional even absent a particularized suspicion due to the government's compelling interest in reducing the influx of illegal aliens, the Border Patrol's inability to do so at the border, and the minimal harm to the traveller.[678] In *Michigan Department of State Police v. Sitz*,[679] the Court found that even if only 1.5% of the drivers stopped were drinking, the governmental interest was great enough to justify the intrusion of a highway checkpoint.[680] *Sitz* used a three-prong test[681] requiring (1) a

---

[676] The ECPA presumably protects against the warrantless interception and recording of encrypted communications even when the public servants recording the message lack the capability to decrypt it. Otherwise, public servants would routinely be able to record encrypted messages and then decrypt them if they were later able to amass sufficient evidence to convince a judge to issue a valid warrant. Any other construction of the ECPA would make it almost a dead letter.

In this perspective, the Fifth Circuit's decision in Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994), is troubling but inapposite. The Fifth Circuit imposed a narrow construction on the ECPA prohibition against "intentionally intercepting" e-mails, 18 U.S.C § 2511(1)(a) (1988), to exclude e-mail communications residing on a computer bulletin board but not yet received by the intended recipient. In the Fifth Circuit's stunted view, an "intercept" can only occur if the communication is overheard during transmission. *Id.* at 461-62. The court held that the capture of an unread e-mail stored on a bulletin board is governed by the less stringent provisions of Title I of the ECPA, which covers the electronic storage of messages. *See id.* at 461-63.

The *Steve Jackson* decision is worrisome because it suggests that courts will interpret the ECPA narrowly. It is inapposite because the recording of an encrypted communication during transmission clearly falls under Title II of ECPA. *See also id.* at 462 n.7 (explaining that a search warrant would be required to obtain access to contents of a stored electronic communication).

[677] 428 U.S. 543 (1976).

[678] *See id.* at 558-67.

[679] 496 U.S. 444 (1990).

[680] *See id.* at 455.

weighing of the gravity of the public concerns served by the seizure, (2) some empirical evidence that the program was effective,[682] and (3) a weighing of the severity of the interference with individual liberty.[683]

The car metaphor will no doubt have appeal beyond law enforcement if only because it is already commonplace to talk about the Internet as a highway, complete with "on-ramps," "fast lanes," and "maps." Perhaps it is time to abandon these convenient phrases. If the car metaphor prevails, there will be far fewer constitutional rights in cyberspace than if any other metaphor comes to dominate.[684]

b. *"Language"*

A cipher resembles a foreign language. Indeed, during World War II, the U.S. Navy used speakers of obscure Native American languages to exchange radio messages that could not be understood by the Japanese.[685] A federal law requiring that English be the sole mode of communication for telephones or e-mails would be unconstitutional on First Amendment grounds and would violate the Equal Protection Clauses of the Fifth and Fourteenth Amendments.[686] If one accepts the analogy, it follows that no

---

[681] The test originated in Brown v. Texas, 443 U.S. 47 (1979).

[682] *See* 496 U.S. at 454. The original formulation of the test weighed the degree to which the procedure advances the public interest, but the *Sitz* Court appears to have lowered its scrutiny of this factor and to have looked instead to some evidence of effectiveness. *See id.* at 454-55.

[683] *See Brown*, 443 U.S. at 50-51.

[684] *Cf.* California v. Acevedo, 500 U.S. 565 (1991) (discussing the "automobile exception" to the Fourth Amendment).

[685] *See* KAHN, *supra* note 6, at 549-50.

[686] *See, e.g.*, Farrington v. Tokushige, 273 U.S. 284, 298-99 (1927) (discussing the constitutionality of regulations aimed at foreign language schools); Yu Cong Eng v. Trinidad, 271 U.S. 500, 525 (1926) (same); Bartels v. Iowa, 262 U.S. 404, 411 (1923) (finding unconstitutional a state statute prohibiting the teaching of foreign languages in public schools); Meyer v. Nebraska, 262 U.S. 390, 400 (1923) (recognizing a parent's right to determine the language to be spoken by her child); Yniguez v. Arizonans for Official English, 1994 U.S. App. LEXIS 37650, *30-*47 (9th Cir. Jan. 17, 1995) (amending 1994 U.S. App. LEXIS 34195 (9th Cir. Dec. 7, 1994)) (holding that Article XXVIII of the Arizona constitution, which requires that English be used for all official business, violates the First Amendment of the U.S. Constitution); Asian Am. Business Group v. City of Pomona, 716 F. Supp. 1328, 1330-32 (C.D. Cal. 1989) (holding that an ordinance requiring one-half of the space of a foreign alphabet sign to be devoted to English alphabetical characters violated First Amendment free speech rights and the Equal Protection Clause); *see also* Antonio J. Califa, *Declaring English the Official Language: Prejudice Spoken Here*, 24 HARV. C.R.-C.L. L. REV. 293,

cryptosystem may be outlawed. Nor, continuing the analogy, can the government require that users provide it with a translation of their messages. Not only would this have Fifth Amendment implications,[687] but it would chill free speech.[688]

Although a cipher resembles a foreign language, it is not

330-46 (1989) (arguing that English-only laws violate the Equal Protection Clause); Donna M. Greenspan, *Florida's Official English Amendment*, 18 NOVA L. REV. 891, 908-16 (1994) (arguing that a lack of enforcement saves the constitutionality of Florida's Official English amendment, and warning that some day Spanish-speaking citizens might seek to use similar laws against English speakers); Joseph Leibowicz, *The Proposed English Language Amendment: Shield or Sword?*, 3 YALE L. & POL'Y REV. 519, 542-50 (1985) (arguing that the English Language Amendment should be rejected because it embraces a pure form of Anglo-conformity and uses a language issue as a weapon against those already the objects of cultural or racial prejudice); Wendy Olson, *The Shame of Spanish: Cultural Bias in English First Legislation*, 11 CHICANO-LATINO L. REV. 1, 23-28 (1991) (arguing that English-only laws stigmatize language minorities and violate their constitutional rights to equal protection and privacy); Juan F. Perea, *Demography and Distrust: An Essay on American Languages, Cultural Pluralism, and Official English*, 77 MINN. L. REV. 269, 356-57 (1992) (asserting that official English laws should be subject to heightened scrutiny); Hiram Puig-Lugo, *Freedom to Speak One Language: Free Speech and the English Language Amendment*, 11 CHICANO-LATINO L. REV. 35, 44-46 (1991) (arguing that English-only laws would be unconstitutional); Michele Arington, Note, *English-Only Laws and Direct Legislation: The Battle in the States over Language Minority Rights*, 7 J.L. & POL. 325, 339-42 (1991) (arguing that official-English laws should be interpreted narrowly rather than as broad restraints on bilingual programs); Note, *"Official English": Federal Limits on Efforts to Curtail Bilingual Services in the States*, 100 HARV. L. REV. 1345, 1352-56 (1987) (arguing that English-only laws violate the Equal Protection Clause and unconstitutionally limit the access of language minorities to the political process); Leo J. Ramos, Comment, *English First Legislation: Potential National Origin Discrimination*, 11 CHICANO-LATINO L. REV. 77, 92-93 (1991) (arguing that language discrimination is facial discrimination deserving strict scrutiny); Carol Schmid, Comment, *Language Rights and the Legal Status of English-Only Laws in the Public and Private Sector*, 20 N.C. CENT. L.J. 65, 72-76 (1992) (analyzing issues raised by English-only laws).

[687] I have been unable to find a single criminal case in which the government has attempted to force a defendant to translate her message. There are cases in which the government provides translations of an eavesdropped conversation and then in effect challenges the defendant to explain what is wrong with the government's incriminating rendition. *See, e.g.*, United States v. Briscoe, 896 F.2d 1476, 1490-93 (7th Cir. 1990) (involving a translation from a Nigerian dialect). Similarly, some courts have held that parties cannot be required to translate foreign-language documents as part of civil discovery governed by the Federal Rules of Civil Procedure. *See, e.g.*, *In re* Korean Airlines Disaster of Sept. 1, 1983, 103 F.R.D. 357, 357-58 (D.D.C. 1984) (denying a motion to direct Korean Airlines to provide English translations of Korean documents). The Supreme Court has held that in cases under the Hague Evidence Convention a federal court may require a party providing documents to provide translations as well as descriptions of documents. *See* Société Nationale Industrielle Aérospatiale v. United States Dist. Court for the S. Dist. of Iowa, 482 U.S. 522, 546 (1987).

[688] *See supra* part III.A.2.

identical. No one can speak in DES without mechanical aids, and no one can understand a DES-encrypted message if they do not understand the language of the plaintext. Cryptologist Dorothy Denning argues that these differences are so great that in some important sense encrypted speech "is not speech."[689] As Denning notes, languages have semantic blocks such as words, phrases, sentences, or ideograms that "carry" meaning and that can be manipulated, but ciphertext has no such blocks.[690] Also, Denning argues, all languages share the property that thoughts, emotions, beliefs, requests, offers, and concepts can be expressed without knowledge of any other language.[691] In contrast, ciphertext not only needs to be decrypted to be understood, but the recipient must understand the language of the plaintext in order to comprehend the message.[692]

Existing First Amendment jurisprudence provides guidance that helps determine whether these differences between enciphered communications and ordinary language speech should be considered legally significant.[693] The First Amendment protects communicative acts, not specific modes of communication.[694] The First

---

[689] Dorothy E. Denning, Encrypted Speech Is Not Speech 1 (Jan. 16, 1994) (unpublished manuscript, on file with author). In addition to the items discussed in the text, Denning argues that all languages are capable of direct translation to all other languages without the intermediation of a third language, but that a ciphertext, which often consists of strings of ones and zeros, must first be decrypted to its plaintext before being translated into another language. *See id.* In an e-mail to the author, Professor Denning qualified her claim that encrypted speech "is not speech" by adding: "My conclusion was that encryption must be regarded as a manner of speech rather than speech (or manner of expression) in a more fundamental sense. This, of course, does not rule out its protection." E-mail from Dorothy Denning, Professor and Chair, Computer Science Department, Georgetown University, to Michael Froomkin (Dec. 7, 1994) (on file with author).

[690] Denning, *supra* note 689, at 1-3. Denning also argues that all languages have syntactic malleability—that is, the ability to use semantic building blocks in different orders and combinations that produce meanings—but that ciphertext lacks this property because reordering the ones and zeros will usually produce gibberish. *See id.*

[691] Because American English, like many languages, borrows heavily from other languages, this statement presupposes a very robust conception of the parameters of a living language.

[692] *See* Denning, *supra* note 689, at 1-3.

[693] In considering the extent to which ciphertext resembles speech protected by the First Amendment, I am not assuming that it is so protected. To invoke the First Amendment directly to resolve the constitutional status of ciphertext would be to beg the question that the invocation of the "language" metaphor is supposed to answer. The argument in the text seeks instead to use First Amendment cases to classify differences as relevant to whether a communication is protected speech or not.

[694] *See* Texas v. Johnson, 491 U.S. 397 (1989) (holding that burning the American

Amendment protects many communicative acts that do not use words including photographs, pictures, nude dances,[695] and silent protest.[696] Although they do not use words, these protected communications do have messages. They have semantic units and referents of the type described by Roland Barthes and others.[697] Indeed, the Supreme Court recently reaffirmed the importance of the connection between an unspoken assertion of the speaker's identity and the communicative content of the message. In *City of Ladue v. Gilleo*,[698] the Court held that an ordinance prohibiting the display of signs in the front yard of a house violated the resident's right to free speech as "the identity of the speaker is an important component of many attempts to persuade."[699] Similarly, there is no reason to believe that the First Amendment is concerned with the degree to which a communicative system depends upon another or stands alone.[700] If the First Amendment protects works of art so obscure that they can only be understood by their creator,[701] it can equally well be applied to protect encrypted speech. Thus, from a First Amendment standpoint, the differences between ciphertext and ordinary language identified by Denning are irrelevant to

---

flag for expressive reasons falls under the protection of the First Amendment); Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503 (1969) (holding that the First Amendment protects the wearing of an armband for expressive reasons); United States v. O'Brien, 391 U.S. 367 (1968) (finding that the First Amendment safeguards the burning of a draft card for expressive reasons); Stromberg v. California, 283 U.S. 359 (1931) (recognizing that the display of a red flag was protected speech).

[695] *See* Doran v. Salem Inn, Inc., 422 U.S. 922, 932 (1975). *But see* Barnes v. Glen Theatre, Inc., 501 U.S. 560 (1991) (qualifying *Doran*).

[696] *See* Brown v. Louisiana, 383 U.S. 131 (1966).

[697] *See generally* BARTHES, S/Z, *supra* note 671; HOLDCROFT, *supra* note 671.

[698] 114 S. Ct. 2038 (1994).

[699] *Id.* at 2046.

[700] *Cf.* Texas v. Johnson, 491 U.S. 397, 404 (1989) (stating that whether particular conduct is protected by the First Amendment depends on "whether '[a]n intent to convey a particularized message was present, and [whether] the likelihood was great that the message would be understood by those who viewed it[]'" (quoting Spence v. Washington, 418 U.S. 405, 410-11 (1974))).

[701] Commentators disagree as to whether the First Amendment protects communications or communicative intent. *Compare* Frederick Schauer, *Speech and "Speech"–Obscenity and "Obscenity": An Exercise in the Interpretation of Constitutional Language*, 67 GEO. L.J. 899, 918 (1979) ("[A]ny rational justification for the principle of free speech requires both a communicator and an intended object of the communication.") *with* Melville B. Nimmer, *The Meaning of Symbolic Speech Under the First Amendment*, 21 UCLA L. REV. 29, 36 (1973) ("The right to engage in verbal locutions which no one can hear and in conduct which no one can observe may sometimes qualify as a due process 'liberty,' but without an actual or potential audience there can be no first amendment speech right.").

whether a communication is protected speech.

From the viewpoint of the language metaphor, the most troubling difference between ciphertext and classic protected speech is that, in the case of ciphertext, a mechanical aid is required to both create and comprehend the message. This difficulty should not be exaggerated—metaphors, after all, are invoked when things are not identical, not when they are precisely the same. It is unlikely that the mechanical aid would appear as troublesome if, instead of a cryptographic system, the device in question were a prosthetic device, such as a voice synthesizer or an eye-movement operated computer.[702] In the case of these prosthetic devices, one would not expect to find arguments that the communication emanating from the device, or the signals used to operate the device, were any less entitled to First Amendment protection than ordinary speech. Again, the ciphertext example is not identical because the parties to the communication presumably have alternate forms of communication available to them, but this just underlines the fact that it is not the mechanization of the communication that ought to be the stumbling block. As new technologies such as voice recognition become commonplace, one would not expect to see arguments that the speech is somehow less protected while in the binary form that intermediates between sound waves and text, even if the author could have used a pencil instead of speaking to a computer. In any event, because a work of art requiring computer animation or computer-aided virtual reality would depend critically on the assistance of a machine, it would clearly be entitled to the same First Amendment protections as a painting.

Encrypted speech is not exactly an ordinary language, but it is similar to what we ordinarily mean by language. Moreover, most of the differences are not the ones that usually matter in the First Amendment context. The most significant difference between encrypted speech and ordinary speech is the role of a machine. Indeed, the encrypted communication much resembles the telephone call, as voice is translated into a ciphertext (an electrical or fiber-optical signal) that is transmitted to the recipient who then

---

[702] "Seen as a prosthetic device, the personal computer extends the limits of the individual human body, whether within the privatized microworlds of computer simulations, or through the interactive exchange of messages across global computer networks." Deborah Heath, Computers and Their Bodies: Sex, War and Cyberspace 1 (1992), *available online URL* gopher://gopher.cpsr.org:70/00/cpsr/gender/clark/Heath.Deborah.

decrypts it (plays it on a speaker). Telephone calls are subject to wiretaps not because a machine is involved in the communication, but rather because once public servants have obtained the appropriate warrant, the signals are in the same position as unmechanized speech inside the home.

Rejection of the language metaphor might lead to undesirable consequences. If the government were able to require that users of strong cryptography ensure the government's ability to decrypt their messages, it might be only a small step to imposing limits on the use of languages other than English.[703] Would the last two speakers of a dying language be required to provide translations of their conversations if the government charged that they were conspiring in it? Such a rule would be as difficult to apply as it might be difficult to distinguish among impenetrable slang or strange accents, a language, and a code.

2. Focus on Exclusion

Just because somebody wishes to hide something does not mean that the Constitution necessarily protects it. If desire sufficed to produce exclusive control over information, successful prosecutions would be rare. Conversely, just because the government would find it convenient to know something about an individual does not mean that the individual has any duty to make the information easily accessible.[704] In mediating between these extremes, the Supreme Court has given at least lip service to the subjective and objective reasonableness of the individual's desire to block the state's access to information. Reasonableness of expectations is a particularly manipulable socially constructed term because the courts' decisions are an important determinant of what is reasonably expected. If, despite this, one grants that the idea of reasonable expectations has some exogenous content, then the courts' willingness to protect strong cryptography against government control is likely to be influenced by the extent to which judges find something familiar and reasonable in the act of encrypting a message. Cryptography that feels like a PIN number used to access cash machines will be treated differently from cryptography that feels like the tool of drug dealers and terrorists.[705]

---

[703] *See supra* text following note 468; *supra* text accompanying note 686.

[704] The important qualifications to this statement, including regulatory searches, valid subpoenas, and searches with valid warrants appear *supra* part III.B.

[705] A number of participants in the cypherpunks mailing list, notably cypher-

a. *"Safe"*

A cipher is armor around a communication much like a safe is armor around a possession. A person who puts something in a safe to which they have the only key or combination surely has both a subjective and objective reasonable expectation of privacy regarding the contents.

Simply putting something into a safe does not, however, ensure that it is beyond the law's reach. It is settled law that a criminal defendant can be forced to surrender the physical key to a physical safe, so long as the act of production is not testimonial.[706] Presumably a similar rule compelling production would apply to a criminal defendant who has written down the combination to a safe on a piece of paper. There appears to be no authority on whether a criminal defendant can be compelled to disclose the combination to a safe that the defendant has prudently refrained from committing to writing, and in *Fisher v. United States*,[707] the Supreme Court hinted that compelling the disclosure of documents similar to a safe's combination might raise Fifth Amendment problems.[708] Perhaps the combination lock problem does not arise because the police are able to get the information from the manufacturer or are simply able to cut into the safe. These options do not exist when the safe is replaced by the right algorithm. Although brute-force cryptography is a theoretical possibility,[709] neither safe cracking, nor number crunching, nor an appeal to the manufacturer is a practical option when the armor is an advanced cipher. The recently released Federal Guidelines for Searching and Seizing

---

punks' co-founder Eric Hughes, have argued in their postings to the list that cryptography can only become safe from regulation if it becomes ubiquitous. This analysis suggests that they are onto something. If nothing else, the push to provide ubiquitous and user-friendly cryptography could serve to shorten the "cultural lag," for court decisions defining the legal regime for a new technology often are made before the technology is well-understood by the public or judges. *See* Diane C. Maleson, *The Historical Roots of the Legal System's Response to Nuclear Power*, 55 S. CAL. L. REV. 597, 617-18 (1982) (giving as an example of "cultural lag" the issue of nuclear power plant safety).

[706] *See* Doe v. United States, 487 U.S. 201, 210 n.9 (1988) (analogizing to the forced production of a strongbox key).

[707] 425 U.S. 391 (1976).

[708] *See id.* at 409 (stating that the Fifth Amendment ordinarily protects against the compulsion to "restate, repeat, or affirm the truth of the contents of documents sought").

[709] *See infra* Technical Appendix, part A.

Computers[710] suggest that "[i]n some cases, it might be appropriate to compel a third party who may know the password (*or even the suspect*) to disclose it by subpoena (with limited immunity, if appropriate)."[711]

Even if ciphertext is analogous to a document in an uncrackable safe whose combination has never been written down, there are important differences between a paper in a vault and an encrypted e-mail. A safe is a container into which people put things and take them out again, preserving the contents over time by keeping unauthorized persons from having access to them.[712] Ordinarily, a safe stays put. E-mails usually move around.

Current law on moving containers is not very friendly towards privacy. The Supreme Court has stated that "some containers (for example, a kit of burglar tools or a gun case) by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance."[713] That, at least, can never be the case with an encrypted message, because the external appearance of ciphertext gives no clue as to its content.

The moving safe begins to look a little like luggage.[714] Intuitively, the privacy interest in a safe seems greater than the privacy interest in luggage, which is perhaps fortunate because the privacy interest in luggage has been shrinking towards the vanishing point.[715] Ordinary luggage can be searched without a warrant upon reasonable suspicion.[716] There appear to be no recent

---

[710] *See* 56 Crim. L. Rep. (BNA) No. 12, at 2023 (Dec. 21, 1994).

[711] *Id.* at 2038 (emphasis added). It is difficult to see, however, how under the Fifth Amendment limited immunity could be given to the suspect without preventing the prosecution from using any information directly resulting from the use of the password.

[712] Words frequently achieve the same effect with regard to the meanings they "carry," but that is not, one hopes, their primary purpose.

[713] Arkansas v. Sanders, 442 U.S. 753, 764-65 n.13 (1979). What a kit of burglar tools looks like, or how its looks differ from an ordinary tool box's, the Supreme Court did not explain.

[714] A safe on the move also resembles an armored car. If so, it is constitutionally unsafe, compared to the stationary safe, because there seems little likelihood of an armored car exception to the Fourth Amendment's automobile exception. *See supra* note 675 and accompanying text.

[715] *See* California v. Acevedo, 500 U.S. 565, 575 (1991) ("Law enforcement officers may seize a container and hold it until they obtain a search warrant.").

[716] *See id.* at 575 (stating that "the police often will be able to search containers without a warrant, despite the *Chadwick-Sanders* rule, as a search incident to a lawful arrest"). The prior rule recognized a privacy interest in luggage. *See* United States v. Place, 462 U.S. 696, 706-07 (1983) (citing United States v. Chadwick, 433 U.S. 1,

reported cases of police forcing a combination lock on luggage without either consent,[717] a warrant, or an alert from a drug-sniffing dog.

The privacy interest in locked luggage is insufficient to protect the owner against brief detentions of her property, in order to permit a dog sniff.[718] According to the Supreme Court, the sniff is not a Fourth Amendment "search" because the suitcase remains closed during the test, the dog discloses only the presence or absence of narcotics and cannot reveal the contents of the suitcase, and the "canine sniff" is the least intrusive method of ascertaining the presence of narcotics in the baggage.[719]

A sniff has some similarities to the investigation of a LEAF—low intrusion, bag/message remains closed/encrypted during investigation, and the investigation discloses nothing else about the contents of the bag/message. Like a dog alert, detection of an invalid LEAF could tell police that the message has been encrypted with unescrowed cryptography. Unlike dog alerts, LEAF-sniffing will prove generally unreliable because preencrypting a message with another cipher will hide the contents while presenting a valid LEAF for the world to see.[720]

Overall, the safe analogy is appealing. Unfortunately, it either

---

13 (1977) for the proposition that persons possess "a privacy interest in the contents of personal luggage that is protected by the Fourth Amendment"); *see also* United States v. Ross, 456 U.S. 798, 824 (1982) (expanding the warrantless search doctrine under Carroll v. United States, 267 U.S. 132, 153 (1925), to containers in cars upon probable cause); Arkansas v. Sanders, 442 U.S. 753, 764 (1979) (finding luggage to be a common "repository for personal items" inevitably associated with an expectation of privacy), *rev'd sub nom.* California v. Acevedo, 500 U.S. 565 (1991); United States v. Chadwick, 433 U.S. 1, 13 (1977) (stating that movable luggage has a greater reasonable expectation of privacy than automobile), *rev'd sub nom.* California v. Acevedo, 500 U.S. 565 (1991).

[717] Or at least testimony from which a court might infer consent. *See, e.g.*, United States v. Cox, 762 F. Supp. 145 (E.D. Tex. 1991) (concluding that by unlocking the combination lock of a suitcase, the defendant consented to a search); United States v. Miller, 442 F. Supp. 742, 748 n.5, 753 (D. Me. 1977) (stating that the fact that an officer told the suspect that a lock would be opened with or without his help did not vitiate consent); *cf. supra* note 366 and accompanying text (suggesting that the intelligence of criminals is not to be overestimated).

[718] How brief is unclear. Ninety minutes is too long. *See Place*, 462 U.S. at 709-10 (stating that the Court has "never approved a seizure of the person for the prolonged 90-minute period involved here").

[719] *Id.* at 707 ("We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure.").

[720] On whether the LEAF is inside or outside the message for ECPA purposes, see *supra* notes 330-36 and accompanying text.

maps the problem onto an equally unsettled area of law or collapses back to another form of the conduit metaphor.[721] It also has the moderate defect of being vulnerable to technical changes, although for the foreseeable future high-level encryption will remain far, far easier than brute-force decryption. It may be, however, that despite the potential for instability after the next technological or cryptographic revolution, the absence of law relating to combination locks without written combinations (the case most analogous to a strong cipher with a secret passphrase) creates an opportunity to make new law unencumbered by the baggage of the Supreme Court's luggage precedents. There is no obvious reason why a person's privacy interest in the contents of a safe, or a ciphertext, should decrease sharply because the object is in transit, and it would not be difficult to have the law reflect that reasonable expectation.

b. *"House"–Where Messages Come From*

Just as the car is a place where constitutional protections are near their weakest, the house is where they approach their strongest. The difference between the house and car metaphors is perhaps best illustrated by *California v. Carney*,[722] in which the Court had to decide whether a mobile home was a house or a car. If it were a house, then it could only be searched with a warrant; if a car, then no warrant was needed. The Court held that a moving RV is a car for Fourth Amendment purposes, but left open the case of a mobile home that is up on blocks.[723]

The Supreme Court's first encounter with wiretapping produced a five-to-four decision holding that a wiretap was neither a search nor a seizure because it took place outside the home and did not interfere with the transmission of the message. "The reasonable view," Chief Justice Taft announced, "is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside"; having left the sanctity of the home, those messages and those wires "are not within the

---

[721] Once one considers movement, the "safe" begins to look like another conduit metaphor, in which meanings are placed into a safe/cipher that "holds meaning" and then "conveys" the meaning to another.

[722] 471 U.S. 386 (1985).

[723] *See id.* at 394 & n.3. In Soldal v. Cook County, Ill., 113 S. Ct. 538, 549 (1992), the Supreme Court treated the movement of a trailer home affixed to a foundation as a seizure, but this would apply whether the object was a home or a car.

protection of the Fourth Amendment."[724] The majority's first encounter with the law enforcement aspects of the telephone treated it as a familiar thing: an instrument to send a message out into the world, to meet whatever fate might befall it once it was outside the constitutionally protected zone of the home—a protection that relied in large part on the homeowner's property interest in the residence.[725] Justice Brandeis's dissent relied instead on *Boyd*'s holding that the Fourth Amendment prevents the government from forcing a person to produce an incriminating document.

Katz abandoned the idea that the test for Fourth Amendment protection rested on location. "[T]he Fourth Amendment," Justice Stewart wrote, "protects people, not places,"[726] and it thus protected a conversation originating in an enclosed public telephone booth. Or rather, as Justice Harlan put it in his concurrence, the Fourth Amendment protects a person who has "exhibited an actual (subjective) expectation of privacy" and the expectation is "one that society is prepared to recognize as 'reasonable.'"[727] Justice Stewart cautioned that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[728] Dissenting in *Katz*, Justice Black accused the majority of choosing "to rely on their limited understanding of modern scientific subjects in order to fit the Constitution to the times and give its language a meaning that it will not tolerate."[729] His complaint was that Justice Harlan's concurrence, and by implication the majority's opinion, argued that it was "'bad physics'"[730] to maintain the rule originating in *Olmstead v. United States* that electronic eavesdropping was not a search.[731] Justice Black believed that the Fourth Amendment's protection of the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" connoted the idea of "tangible things with size, form, and weight, things

---

[724] Olmstead v. United States, 277 U.S 438, 466 (1928).

[725] The exception for messages entrusted to the Postal Service, deriving from Ex parte Jackson, 96 U.S. 727, 733 (1877), which held that the Fourth Amendment protects sealed letters in the mail, was explained as owing to the government's control of the mails. *See also* United States v. Chadwick, 433 U.S. 1, 10 (1977) (reaffirming application of the Fourth Amendment to mails).

[726] Katz v. United States, 389 U.S. 347, 351 (1967).

[727] *Id.* at 361 (Harlan, J., concurring).

[728] *Id.* at 352.

[729] *Id.* at 372 n.* (Black, J., dissenting).

[730] *Id.*

[731] *Id.* (noting Olmstead v. United States, 277 U.S. 438 (1928)).

capable of being searched, seized, or both" and that an overheard conversation, even on a wire, was none of these.[732]

In fact, it was Justice Black's physics that were faulty. Electrons have size, form, and mass, as do digitized and encrypted messages. Yet despite its questionable physics, Justice Black's legal conclusion appears to be gaining support: since, *Katz*, the Fourth Amendment, and its emanations have been read more and more narrowly. The Court has examined expectations of privacy that often seem greater, and more objectively reasonable, than those of a telephoner in a public phone booth, but has nonetheless found those expectations—when held by guilty parties—to be unreasonable.[733] Similarly, *Boyd* has been whittled away to the point that what vitality it retains is limited to personal, noncommercial papers, and even that is now in doubt. The rationale for *Boyd*'s original holding has been effectively abandoned.[734]

In the place of *Katz* and *Boyd*, the Supreme Court has substituted an anemic form of the property theory of the Fourth Amendment that animated the majority in *Olmstead* and Justice Black's dissent in *Katz*, a theory that in its new form rarely seems to extend outside the curtilage of the home.[735] Although not stated as a general principle, as a practical matter the *Katz* test has come to depend on the objective reasonableness of an expectation of privacy,[736] and the Court has routinely turned to legal or administrative sources to define the parameters of reasonableness[737]—

---

[732] 389 U.S. at 365 (Black, J., dissenting).

[733] *See supra* text accompanying note 656 (noting that government has prevailed in most of the recent search and seizure cases before the Supreme Court).

[734] *See supra* text accompanying notes 467-70 (describing ways in which the *Boyd* decision has been limited).

[735] The Supreme Court's test for resolving extent-of-curtilage questions demonstrates the resonance of the idea of "house": the area claimed to be curtilage will be placed under the home's "umbrella" of protection if intimately tied to the home by proximity, an enclosure surrounding the home, the nature and uses to which the area is put, and the steps taken by the resident to protect the area from observation by passersby. *See* United States v. Dunn, 480 U.S. 294, 301 (1987) (listing the four factors with which the curtilage question should be resolved).

[736] *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (arguing that the privacy "analysis must . . . transcend the search for subjective expectations"); Terry v. Ohio, 392 U.S. 1, 19 (1968) (noting that "the central inquiry under the Fourth Amendment [is] the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security"); *see also Dunn*, 480 U.S. at 300 ("[T]he extent of curtilage is determined by factors that bear upon whether an individual reasonably may expect that the area in question should be treated as the home itself.").

[737] The same Court that looked to community standards in order to determine the

except when it ignores them.[738] Thus, for example, once trash is placed on the curb to be picked up, the property interest in it is gone, and the trash is up for grabs.[739] If it is lawful to fly over a property, it is objectively unreasonable for the owner to expect that the property was safe from aerial inspection regardless of the frequency of such flights or community standards of reasonableness, whatever those may be.[740] But despite the trespass by the observer, there is no reasonable expectation of privacy against ambulatory police intrusion into an "open" field, though surrounded by woods, behind a locked gate with a "No Trespassing" sign, because the field is open to view.[741]

Katz still applies to its facts, which involved a wiretap of a telephone call from an enclosed area. And the home clearly retains a special status, because in *United States v. Karo*[742] warrantless monitoring of a beeper placed by a government informant became unconstitutional at the point where it "reveal[ed] a critical fact about the interior of the premises that the Government . . . could not have otherwise obtained without a warrant."[743] But given the Court's record with reasonable expectations, the reason that *Katz* is still good law seems to have more to do with the existence of Title III than any constitutional principle. It has come to the point where the citizen's privacy interests might be better protected if the

---

line between obscenity and legal pornography has not chosen to apply this amorphous standard to determine objectively reasonable expectations of privacy.

[738] For a fuller description, see Daniel B. Yeager, *Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. CRIM. L. & CRIMINOLOGY 249 (1993) (surveying and analyzing the Court's Fourth Amendment jurisprudence).

[739] *See* California v. Greenwood, 486 U.S. 35, 39-40 (1988) ("An expectation of privacy does not give rise to Fourth Amendment protection, however, unless society is prepared to accept that expectation as objectively reasonable.").

[740] *See* Florida v. Riley, 488 U.S. 445, 451-52 (1989) (plurality opinion) ("[T]here is nothing . . . to suggest that helicopters flying at 400 feet are sufficiently rare in this country to lend substance to respondent's claim that he reasonably anticipated that his greenhouse would not be subject to observation from that altitude."); *see also* California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding valid a warrantless aerial surveillance of yard enclosed by a 10-foot fence).

[741] *See* Oliver v. United States, 466 U.S. 170, 179 (1984) (finding that "[i]t is not generally true that fences or 'No Trespassing' signs effectively bar the public from viewing open fields in rural areas"); *see also* United States v. Dunn, 480 U.S. 294 (1987) (refining the concept of a protected zone within curtilage); *Ciraolo*, 476 U.S. at 215 (finding a reasonable expectation of privacy lacking with regard to a property surrounded by a 10-foot fence in an age in which private and commercial flight in public airways is routine).

[742] 104 S. Ct. 3296 (1984).

[743] *Id.* at 3303.

discredited property-based theory of *Olmstead* were revived instead of reviled.[744] Coincidentally, the development of mass-market strong cryptography means that the property theory, combined with a computer or a scrambler telephone, produces a level of constitutionally protected communications privacy comparable to the original *Katz* standard.[745] Today, with the right cryptography, it no longer matters as much if *Katz* is narrowed or overturned, at least as far as communications privacy is concerned.[746] Now there is something that the citizen can do, inside the home, before a message is sent out on its vulnerable journey throughout the world.

The value of the legal protections that can pertain to the home if based on a property theory like that in *Olmstead* should not be overstated. So long as we hold to current conceptions of the home, as a physical structure with walls and sometimes a curtilage too, the interconnections between homes will continue to be classified as "outside" the "house." As a result, regulations, including a ban on the use of unescrowed strong cryptography in communications that leave the house, remain a real possibility.

The "house" metaphor may provide some protection against the complete reversal of *Boyd*, depending on whether a court could compel the production of a key that had not been committed to paper. If the court were unwilling to do this, say on Fifth Amend-

---

[744] *See* Yeager, *supra* note 738, at 252-53; Heather L. Hanson, Note, *The Fourth Amendment in the Workplace: Are We Really Being Reasonable?*, 79 VA. L. REV. 243, 262-73 (1993) (suggesting a return to a property rights basis for privacy in the workplace); *see also* Soldal v. Cook County, Ill., 113 S. Ct. 538, 543-45 (1992) (explaining that the Fourth Amendment protects property interests as well as privacy interests). *But see* Rawlings v. Kentucky, 448 U.S. 98, 105-06 (1980) (refusing to extend constitutional protection in the context of a defendant's ownership interest in illegal drugs by rejecting "the notion that 'arcane' concepts of property law ought to control the ability to claim the protections of the Fourth Amendment"); Kreimer, *supra* note 592, at 89-94 (discussing the virtues of disclosure); Stephen J. Schnably, *Property and Pragmatism: A Critique of Radin's Theory of Property and Personhood*, 45 STAN. L. REV. 347, 378 n.153 (1993) (warning that one danger of the reliance upon a property theory of rights is that the home-as-fortress becomes a refuge for harmful acts that might be prevented by exposure).

[745] The argument in the text has mixed implications for other forms of privacy. Records may be protected to the extent that they are encrypted and that production of the key cannot be compelled. Note that compulsion may be a subpoena, a grand jury inquiry, or even civil discovery instigated by the government on pain of tax forfeiture. *See* Ann L. Iijima, *The War on Drugs: The Privilege Against Self-Incrimination Falls Victim to State Taxation of Controlled Substances*, 29 HARV. C.R.-C.L. L. REV. 101, 127-34 (1994) (describing how records and other information may be compelled by taxing authorities to the detriment of drug dealers).

[746] *See infra* Technical Appendix, part B.

ment grounds, strong cryptography would provide a nearly unbreakable means of protecting one's private papers stored in the home computer.[747]

The decision to classify the cryptographic key as akin to a private paper located in the home also may have interesting legal consequences as the idea of the home evolves. Assumptions about space, about what constitutes the "inside" of a home or an office, may need to be reexamined:

> [I]n the era where people work for "virtual corporations" and conduct personal and political lives in "cyberspace," the distinction between communication of information and storage of information is increasingly vague. The organization in which one works may constitute a single virtual space, but be physically dispersed. So, the papers and files of the organization or individual may be moved within the organization by means of telecommunications technology. Instantaneous access to encryption keys, without prior notice to the communicating parties, may well constitute a secret search, if the target is a virtual corporation or an individual whose "papers" are physically dispersed.[748]

In this vision, the cryptographic key becomes the thing after which it is named and is transformed from a metaphor into the actual key to a virtual—or is that actual?—electronic home or office.[749]

C. *The Power to Choose*

Because the First Amendment case for unfettered cryptography would be the strongest, "language" would seem to be the metaphor of choice for advocates of unfettered privacy, although "safe" is sufficiently unsettled to be turned to any conclusion. "Car" offers the most to public servants concerned with preserving their electronic eavesdropping capability. "House" seems like a fair compromise, because it locks in more limited Fourth Amendment protections. From the viewpoint of law enforcement and intelligence agencies, however, a compromise is almost as bad as a complete loss if it is difficult to distinguish legitimate unescrowed messages from illegitimate ones.

A court, or any other interested party, that might be called upon

---

[747] The full ramifications of this question are beyond the scope of this Article.

[748] DIGITAL PRIVACY AND SECURITY WORKING GROUP, *supra* note 31, at 6.

[749] The Supreme Court's decision in *California v. Carney* suggests that this day is still some ways off. *See* California v. Carney, 471 U.S. 386, 393-94 (1985) (holding that a moving recreational vehicle is a car and not a house).

to select among competing metaphors will naturally be concerned about where they might lead. Widespread cryptography may have social implications that are difficult to predict. Strong privacy may not be to everyone's taste. Secret identities will protect the anonymous hate mailer, the drug dealer, the purchaser of seedy movies, the congenitally shy, and the electronic political pamphleteer with equal efficacy. The implications of anonymous transactions for taxes, product liability, and copyright, to name only a few, remain to be worked out.

Sissela Bok hypothesizes a society in which "everyone can keep secrets impenetrable at will. All can conceal innocuous as well as lethal plans, the noblest as well as the most shameful acts, and hatreds and conspiracies as much as generosity and self-sacrifice. Faces reveal nothing out of turn; secret codes remain unbroken."[750] Although Bok recognizes that some version of such a society "might develop precisely in response to the felt threat from increased [information] transparency,"[751] she views such a society as clearly undesirable because "[i]t would force us to disregard the legitimate claims of those persons who might be injured, betrayed, or ignored as the result of secrets inappropriately kept."[752] Strong protection of cryptography may lead exactly there.

However, the absence of the refuge of digital anonymity may be worse. As identifying data on each of us becomes more voluminous and more easily accessible to government and to private parties,[753] our lives are changed, and not necessarily for the better. Indeed, although law enforcement agencies believe they benefit greatly from their electronic eavesdropping capabilities, it is unclear whether society as a whole enjoys a net benefit when one considers both past abuses and the possibilities for future abuses. To foreclose an option that would give the lie to Justice Douglas's dystopian warning that "[w]e are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from the government"[754] would be a communal confession

---

[750] BOK, *supra* note 2, at 16.

[751] *Id.* at 18.

[752] *Id.* at 28.

[753] *See, e.g.*, GANDY, *supra* note 587, at 15 (noting that the collection, processing, and sharing of information about individuals and groups is widespread and continues to expand); *see also* Kevin Fogarty, *Data Mining Can Help to Extract Jewels of Data*, NETWORK WORLD, June 6, 1994, at 40, 40 (describing the practice of "data mining" by which corporations accumulate and manipulate enormous data bases).

[754] Osborn v. United States, 385 U.S. 323, 341 (1966) (Douglas, J., dissenting).

of lack of trust in our fellows and in ourselves. It is chilling to think we are fully capable of making this confession, and that we may even deserve it.

In making legal judgments about the Constitution and cryptography, one should keep in mind what is possible and what is not. This means that one should consider both the extent to which long-held ideas about the meaning of the Bill of Rights need to be rethought in light of technological changes[755] and that some prohibitions simply are unenforceable. Just as the ITAR have failed to stop the spread of strong cryptography abroad (and the development of indigenous substitutes abroad), so too would any attempt to ban unescrowed cryptography be doomed to failure.[756]

Privacy, constitutional law, and law enforcement are not games. It is unsettling to think that one's rights may turn on the extent to which people are able to find a technological means to defeat what would otherwise be legitimate government action. The good news is that technological change can provide an opportunity to rethink, and perhaps increase the coherence of, some constitutional doctrines. When technology changes social realities, interpretations

---

[755] *See supra* text accompanying notes 582-91. This may give cause to invoke another archetype—Frankenstein's monster.

[756] *See supra* part I.C.1.c.i (discussing the ITAR). A law banning unescrowed cryptography, or even only unescrowed commercial cryptography, would provide some advantages for law enforcement. However, under such a regime it might be easier to prove that someone has used unescrowed cryptography than to prove the offense that the secret message would tend to prove. If the defendant will not decrypt the message, she may still be subject to prosecution for the (lesser?) offense of using unregistered cryptography. Although this smacks of prosecuting Al Capone for tax evasion, it may still be an effective technique.

Defining some types of cryptography as contraband would be another approach to the problem, again one with First Amendment problems. Courts have upheld a variety of contraband statutes, but none affected free speech. For example, courts have upheld statutes banning radar detectors (fuzzbusters). *See generally* Nikolaus F. Schandlbauer, Comment, *Busting the "Fuzzbuster": Rethinking Bans on Radar Detectors*, 94 DICK. L. REV. 783, 785-89 (1990) (listing the jurisdictions which prohibit radar detectors). Statutes banning burglars' tools, such as N.Y. PENAL LAW § 140.35 (McKinney 1988) and FLA. STAT. ch. 810.06 (West 1994), have been upheld also, *see, e.g.*, People v. Atson, 526 N.Y.S.2d 618, 619 (N.Y. App. Div.) (requiring more than "purely circumstantial" evidence to sustain a conviction of possession of burglar's tools), *appeal denied*, 528 N.E.2d 896 (N.Y. 1988); Thomas v. State, 531 So. 2d 708, 709-10 (Fla. 1988) (requiring a specific intent to commit burglary when the state burglary tool statute criminalizes common household tools or devices), as have drug paraphernalia statutes, such as 21 U.S.C. § 863 (Supp. V 1993), *see, e.g.*, Posters 'N' Things, Ltd. v. United States, 114 S. Ct. 1747, 1749 n.5, 1754-55 (1994) (upholding the constitutionality of 21 U.S.C. § 857 (1988), which Congress repealed and replaced in 1990 with the virtually identical § 863).

of the Constitution should recognize the change to the maximum extent the text permits. Thus, although we might be better off today with the *Olmstead* standard than into what the Supreme Court has turned *Katz*, we should not lose sight of the fact that *Olmstead* was wrongly reasoned. Chief Justice Taft's formalistic unwillingness to recognize that a telephone call was different from a message on a billboard or a shouted conversation on a busy street is not an attitude that deserves emulation.

The bad news is that sometimes a technological development is unstoppable. It may be that the Administration intends Clipper only as a delaying action.[757] It may be that a future administration, acting for what seem to be good reasons at the time, will attempt a form of cryptological Prohibition. If so, it will fail as Prohibition failed, as the War on Drugs is failing, and as the ITAR are failing with respect to cryptography.[758]

CONCLUSION

The courts, and to a lesser extent Congress, have yet to come to grips with the legal and social implications of consumer cryptography. As a result, this part of the legal landscape is relatively barren. Irrigation and settlement have begun, however, with the executive branch and the private sector as pioneers. The spacial metaphor itself may be inadequate to describe the information revolution of which consumer cryptography is only a part. In distributed networks such as the World Wide Web, in which information may be one mouse-click on a hypertext link away regardless of where it happens to be physically stored, traditional ideas of distance and mapping may prove greater impediments than guides to understanding.[759] Other concepts, such as density of information, quality, reputation, or reliability may come to predominate.

The executive branch's primary concern has been to accommodate the interests of banks and others who require strong cryptography, while also preserving to the greatest extent possible law enforcement and intelligence capabilities. Noncommercial social implications of cryptography have received relatively little attention.

---

[757] *See supra* text accompanying note 367.

[758] *See supra* part I.C.1.c.i (discussing the ITAR's lack of effectiveness).

[759] *See generally* E-mail from Rishab A. Ghosh to Michael Froomkin (Jan. 11, 1995) (on file with author) (arguing, by quoting from his article in *Asian Age* magazine of January 2, 1995, that in cyberspace "distance—as we usually understand it—disappears").

The private sector's motives are more difficult to summarize, but there has clearly been a demand for cryptographic products, and this demand is expected to grow rapidly.[760]

The executive branch's desire to maintain its ability to eavesdrop on electronic communications at will has driven it to abuse the technical standard-setting process. By manipulating the FIPS procedure, the Clinton Administration has achieved its initial objective of promulgating a standard that is insulated from any meaningful public comment and immune from judicial review. The Administration thus hopes to create a de facto rule where it lacks the statutory authority to create a rule de jure. Despite the seemingly underhanded aspects of the executive branch's behavior, there is no clear evidence that it has failed to comply with existing laws or the Constitution. There is, however, room for doubt, as some of the critical information regarding whether NIST retains its statutorily mandated independent judgment is classified. Congress would be well advised to reassure itself and the public that NIST has complied with the Computer Security Act's requirement that it not delegate decision-making to the NSA. If the NSA is calling the shots, firm persuasion, and perhaps corrective legislation, will be required.

The Administration hopes to coerce acceptance of an escrowed encryption product through its vast purchasing power, but whether this hope can be realized remains unclear. If this attempt fails, the next step may be to seek legislation requiring users of strong cryptography to allow the government some form of access to their cryptographic keys. If, despite what currently seems to be a prevailing opposition to even voluntary key escrow, such a bill were nonetheless to become law, mandatory key escrow would create serious constitutional problems that the courts would have to resolve.

Under current law, the judicial reaction to a hypothetical mandatory key escrow statute would be limited primarily to a balancing test analysis, although private noncommercial users would have a particularly strong Fourth Amendment argument on their side, and a good First Amendment argument as well. Recent history suggests, however, that the government's interest in national security or law enforcement often outweighs the citizen's right to privacy.

---

[760] *See supra* part I.A.

By their nature, balancing tests almost demand that courts give some play to the judge's hopes and, especially, fears. A mandatory key escrow statute would evoke two conflicting sets of fears, one over control and the other over lawlessness, symbolized by the archetypes of Big Brother and the criminal cabal. In the end, the conflict may be decided by the way the courts characterize cryptography. Just as the cryptographic "key" is a metaphor, so too may the choice among possible metaphors determine how much constitutional protection an encrypted message gets. If the courts treat a ciphertext as if it had been written in a foreign language, it will trigger a First Amendment analysis that will result in giving cryptography more protection than if the courts focus on the place where the message is encrypted. If encryption is considered no more than the outer envelope in a message transmission system —essentially a "car" on the information superhighway—it is likely to receive the lowest level of protection.

Encryption has much to offer the commercial, professional, and personal users of telephones, computers, and computer networks. As these and other uses grow, they will breed conflict, some of which will inevitably be brought to the courts. The legal ecology of cyberspace is currently underpopulated, but not for long. Clipper and Capstone are only the first of many attempts by the government, and no doubt others, to protect the status quo from changes that upset long-established power relationships. The choices made in the next few years will shape the evolution of electronic communication, and society in general, for decades to come. It would be sad if cyberspace became the first place that the government required civilians, in peacetime, to structure their private communications to make hypothetical future eavesdropping by law enforcement easier.

TECHNICAL APPENDIX: BRUTE-FORCE CRYPTANALYSIS, PUBLIC-KEY ENCRYPTION AND DIGITAL SIGNATURES

> There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.[761]

Cryptography makes it possible to talk privately even if someone is listening in on your telephone line:[762] you can have a secure communication over an insecure channel. Cryptography also allows you to keep electronic records in a form that is easily accessible to you but inaccessible to snoops, whether siblings or governments. Ironclad protection, however, requires effort.

Part of the art of cryptography consists of choosing an appropriate level of security because, for long texts, the highest-level encryption can be slow even with a computer.[763] If the purpose of the encryption is to keep someone from peeking at the answer to a riddle, printing the answer upside down may be enough. If the purpose is to keep salacious material out of the hands of the lower classes, then Latin was for many years the traditional cipher.[764] If the encryption is used, however, to authenticate wire transfers of funds or to send messages to submarines in wartime, a high-level method is required. In each case, the determination is driven by considerations of the time and effort it takes the sender and receiver to use the system, the resources that a third-party would

---

[761] SCHNEIER, *supra* note 12, at xv.

[762] Note that the best scrambler phones in the world will not protect you from a listening device in your room.

[763] Successful cryptographic systems combine two basic principles: confusion and diffusion. Confusion is nothing more than some form of substitution—letters or, more commonly, sets of information bits representing other letters or information bits in some fashion. Replacing every letter with the one next to it on the typewriter keyboard is an example of confusion by substitution. Diffusion means mixing up the pieces of the message so that they no longer form recognizable patterns. Jumbling the letters of a message is a form of diffusion. Because modern ciphers usually operate at the bit level, many modern cryptographic systems produce confusion and diffusion which depends on every bit of the plaintext. Changing a single character will change the operations performed during encryption, making encryption more difficult, but also more difficult to crack. *See* SCHNEIER, *supra* note 12, at 193; Feistel, *supra* note 7, at 15.

[764] *Cf.* Note, 17 L.Q. REV. 223, 223 (1901) (urging "prudent persons not to write defamatory statements of any kind on postcards, even in the decent obscurity of a learned language").

likely be willing to devote to cracking the system, and the costs of guessing wrong.

The strength of a cryptographic system is usually measured by the amount of effort that would be required to crack it by an enemy who knows the algorithm. This means, absent the discovery of a latent vulnerability in the cipher that allows the attacker to take a mathematical short-cut,[765] a "brute-force" attack in which computers try every possible key.[766] Surprisingly, modern cryptography does not require that the algorithm be kept secret. Indeed, the rule of thumb is that ciphers that depend on keeping the algorithm secret are unreliable.[767] In modern cryptography, only the key, and not the method of encryption needs to remain secret to preserve the security of the message.[768]

The optimal cryptographic system would be easy to use and impossible to crack. The real world imposes tradeoffs between ease of use and vulnerability to attack,[769] although computers now put very powerful cryptography within the reach of anyone who has access to a personal computer (PC). Cryptography can be used to defend against various forms of attack including decryption by third parties, modification of messages, and fabrication of authentic-

---

[765] As we will see, this vulnerability may have been unknown to the cryptographers who designed the cipher, or it may have been inserted intentionally.

[766] The two can sometimes be combined: a mathematical attack might, for example, demonstrate that only certain types of keys need to be tried, thus lowering the computational effort involved.

[767] Algorithms whose security depends on the algorithm being kept secret have "historical interest, but by today's data security standards they provide woefully inadequate security. A large or changing group of users cannot use them, because users will eventually reveal the secret. When they do, the whole security of the system fails. . . . [They are also] trivial to break by experienced cryptanalysts." SCHNEIER, *supra* note 12, at 2.

[768] Ordinarily, in systems using multiple keys, only one of the keys need be kept secret.

[769] The only type of algorithm guaranteed to be secure against all forms of mathematical and brute-force attacks is known as the "one-time pad." A one-time pad is "nothing more than a nonrepeating set of truly random key letters . . . . The sender uses each key letter on the pad to encrypt exactly one plaintext character. The receiver has an identical pad and uses each key on the pad, in turn, to decrypt each letter of the ciphertext." SCHNEIER, *supra* note 12, at 13; *see also* Gardner, *supra*, note 128, at 120 (stating that ciphers that provide "absolute secrecy" are not always used because it is "too impractical"). The critical features of a one-time pad are that the pad must be kept from the enemy, the characters on the pad must be truly random, and the pad must never be used twice. Because large pads are difficult to generate, must be communicated to the recipient in utmost secrecy, and are unwieldy, the one-time pad is difficult to use for anything other than short messages of the highest security. *See* SCHNEIER, *supra* note 12, at 14-15.

looking but spurious messages. A strong cryptographic system protects messages that may be intercepted by an enemy, and also authenticates messages received.

A. *Brute-Force Cryptanalysis*

There are three fundamental ways for a third party to crack a cipher where the algorithm is known but the key is not. First, an enemy can simply steal the key or suborn a key-holder. Second, if the enemy knows the algorithm but not the key, the enemy can try to analyze the cipher, hoping to find a weakness in the algorithm. Some very trusted ciphers have fallen to mathematical analysis, at which point decryption becomes easy.[770] Third, and of particular relevance to modern cryptography, the attacker can mount a "brute-force" attack using computers, perhaps with large numbers of specially optimized chips running in parallel, to try every possible key until the message is decrypted. Finding the sender's key gives the attacker more than the text of a single message; it gives access to all future messages that use the same key. If the sender uses a digital signature, the attacker can forge the sender's signature as well.

If the only (known) way to decrypt a cyphertext is to try every possible key, then a longer key makes for a stronger cipher because a longer key has more possible values. An eight-bit[771] key has 2^8 (256) possible values. A computer would have to try all 256 possible values to be certain of finding the key, although the average number of possible values the computer would have to test before encountering the answer will be only 128. Similarly, if the key is 128 bits long, which is the equivalent of the maximum amount of information in a sixteen-character message on a personal computer,[772] a

---

[770] *See* Eric Bach et al., *Cryptography FAQ (06/10: Public-key Cryptography)* § 6.6 (June 7, 1994), *available online URL* ftp://rtfm.mit.edu/pub/usenet/news.answers/cryptography-faq/part06 ("Historically even professional cryptographers have made mistakes in estimating and depending on the intractability of various computational problems for secure cryptographic properties.").

[771] A bit is a binary unit of information that can have a value of zero or one. Computers organize bits into bytes, often 8, 16, or 32 bits in length. For example, DOS-based personal computers use eight-bit bytes to represent alphanumeric characters.

[772] Although a 16-character message on a PC has 128 bits, most 8-bit-to-a-byte PCs limit the characters that can be represented to fewer than 256 per byte because one bit is used for error-checking. Hence, although the amount of information in a 128-bit key is equal to a 16-character text on a PC, such a text itself would in effect be a much shorter key on most personal computers because an attacker would know that

brute-force attack would require that 2^{128} keys be tested to be certain of finding the key. To put this number in perspective, a computer processing a million keys per second would require about 10^{25} years to complete the task, an amount of time 10^{15} times greater than the estimated age of the universe.[773]

Although 10^{15} times the age of the universe makes for an impressive statistic, it is misleading. Chips capable of trying 256 million keys per second are foreseeable within the decade, and several of these can be harnessed to work together. Trying out keys is often ideally suited to parallel processing. Parallel processing allows a problem to be split up between many computer chips running simultaneously, trying many millions, even billions, of keys per second. The chips need not be part of a single computer: the key-cracking problem can be distributed among large numbers of workstations on a network, with each workstation being only slightly more powerful than today's desktop PCs. Indeed, the problem can be parceled out to several different networks, each communicating with one another only infrequently. A distributed processor of this nature, or a single optimized parallel processor, can try vastly more than a million keys per second, making large keys susceptible to being broken in a reasonable period of time.[774] Parallel processors already on the drawing board might make it possible to break even a 512-bit key at a cost which, although out of reach of the average citizen, would be well within the means of the poorest government.[775] The cryptographer's solution, of course, is to use a longer key.

Exactly how large a key would be vulnerable to an economical brute-force attack is a matter of debate. Advances in computer power continue to make longer and longer keys vulnerable, but the same advances make it easier and cheaper to encrypt and decrypt with longer keys. If one assumes the existence of economically

---

many possible values for certain bits could be ignored. Limiting the possible keys only to lowercase letters and digits would have even more drastic effects: a 56-bit key, which if unconstrained would produce 2^{56} (approximately 10^{16}) possible keys, would be limited to 10^{12} possible keys, making it 10,000 times easier to crack. *See* SCHNEIER, *supra* note 12, at 141.

[773] *See id.* at 7, 129. The universe is estimated to be about 10^{10} years old. *See id.* at 7.

[774] *See* Garon & Outerbridge, *supra* note 26, at 179-81; SCHNEIER, *supra* note 12, at 7.

[775] *See* Ronald L. Rivest, *Responses to NIST's Proposal*, COMM. ACM, July 1992, at 41, 44-45 (estimating that today a 512-bit key can be broken with about $8.2 million worth of equipment, and noting that the cost will continue to shrink).

rational, albeit immoral, attackers seeking to maximize the return on an investment in the computing power needed in order to mount a sustained attack, then high-value secrets are more at risk than low-value ones. They therefore deserve longer keys. No consensus exists as to how much security is enough for high-value secrets, however, and in any case that point is probably well past the security provided by DES.

DES's inventors originally planned to use a 128-bit key, which would have provided 40 sextillion (40,000,000,000,000,000,000,000) times more security, but the NSA persuaded them that 56 bits sufficed.[776] A 56-bit key provides a keyspace of 2^{56}, or 72 quadrillion possible keys.[777] Although this is a very large number, even upon DES's adoption as the U.S. standard in 1977, critics predicted that an optimized computer costing $20 million to build could break an average of two 56-bit DES keys a day. Depreciated over the machine's first five years of service, this would have worked out to only $5000 per solution.[778] This was and is a sum well within the reach of many governments, and the price would be much lower today.[779] DES's inventors estimated that the cost of building such a computer would be closer to $200 million, or $50,000 per key.[780]

If DES had used the 128-bit key originally contemplated, breaking each key would have cost an average of $200 septillion in the 1970s, even using Diffie and Hellman's lowest-cost assumptions. Perhaps as a result of its shorter key, DES is not considered sufficiently secure to protect classified data.[781] Despite suggestions from the NSA that DES might not deserve recertification after 1988,[782] NIST recently recertified DES as suitable for commercial purposes for five more years.[783]

---

[776] *See* BAMFORD, *supra* note 17, at 346-47 (describing the "closed door negotiations" between the NSA and IBM that resulted in the key size reduction from 128 to 56 bits).

[777] *See supra* text accompanying note 108.

[778] *See* BAMFORD, *supra* note 17, at 348; Whitfield Diffie & Martin E. Hellman, *Exhaustive Cryptanalysis of the NBS Data Encryption Standard*, COMPUTER, June 1977, at 74, 74.

[779] *See* Diffie & Hellman, *supra* note 778, at 74 (predicting that the rapidly decreasing cost of computation should have, by 1987, reduced the solution cost to the $50 range); Rivest, *supra* note 775, at 45 (estimating the cost to break a 512-bit key as $8.2 million); *see also* BAMFORD, *supra* note 17, at 348.

[780] *See* BAMFORD, *supra* note 17, at 348-49 (comparing arguments about the cost of a computer that could break a 56-bit key).

[781] *See* FIPS 46-2, *supra* note 106, at 69,348.

[782] *See* H.R. REP. NO. 153 (Part I), 100th Cong., 1st Sess. 18 (1987), *reprinted in* 1987 U.S.C.C.A.N. 3120, 3133.

[783] *See* FIPS 46-2, *supra* note 106, at 69,347. NIST suggested, however, that it may

B. *Public-Key Cryptography*

Before the invention of public-key cryptography in 1976,[784] a sender and receiver who wanted to use a cipher had to agree on a key in order to communicate securely. This method was very burdensome to both parties. First, sender and receiver needed a secure means to transmit the key itself. For example, if you were trying to send a message to your agent behind enemy lines, and you were afraid that the bad guys had cracked your cipher, it was too late to send a coded message saying "the new key is *X*."[785] Second, even if the key was transmitted securely (for example, by handing it to the agent before she left for her mission), the security of a single-key cipher evaporated as soon as the key was compromised. If you wrote the secret key down, someone could have found it; if you did not write it down, either it must have been short or you needed a phenomenal memory. Third, the ever-present danger of key compromise cast a doubt over the authenticity of every message. A third party who had the key could use it to alter messages, or to send fake messages purporting to be from any of the parties who legitimately held the key.

Public-key cryptography solves all of these problems. As a result, public-key cryptography has been described as a "revolutionary technology," which will make routine communication encryption ubiquitous.[786] In a public-key system, each user creates a public key, which is published, and a private key, which is secret.[787]

---

not recertify DES when its current five-year certification expires. *See id.* at 69,350 (noting that in 1998, when the standard will be over 20 years old, NIST will consider alternatives that offer a higher level of security).

[784] For the original papers describing public-key cryptography, see Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IT-22 IEEE TRANSACTIONS INFO. THEORY 644 (1976), and Ralph C. Merkle, *Secure Communication over Insecure Channels*, COMM. ACM, Apr. 1978, at 294. For further information about public-key cryptography, see generally SCHNEIER, *supra* note 12, at 29. More concentrated descriptions can be found in Bach, et al., *supra* note 770, § 6; *RSA Cryptography Today FAQ*, *supra* note 129; and in Whitfield Diffie, *The First Ten Years of Public-Key Cryptography*, 76 PROC. IEEE 560 (1988) (discussing the history of public key cryptography).

[785] This proved to be a real problem during World War II, resulting in the capture of several spy rings. *See* KAHN, *supra* note 6, at 530.

[786] Bach et al., *supra* note 770, § 6.2. Despite the prediction of ubiquity, the fact remains that to date nongovernmental commercial uses of public-key cryptography have been very limited. "It is easy to build a case for buying cryptography futures. . . . Nonetheless, cryptography remains a niche market in which (with the exception of [sales to the government]) a handful of companies gross only a few tens of millions of dollars annually." ACM REPORT, *supra* note 15, at 12.

[787] The ASCII version of the author's public key for his 1024-bit key in Pretty

Messages encrypted with one key can be decrypted only with the other key, and vice-versa. Thus, if Alice wants to send a secure e-mail message to Bob, and they both use compatible public-key cryptographic software, Alice and Bob can exchange public keys on an insecure line. Alice would have to input her plaintext and Bob's public key. The program outputs the ciphertext, which is a stream of characters that looks like garbage to anyone who should happen to see it. When Bob receives the ciphertext, he inputs both it and his private key to his program, which reveals Alice's plaintext.

One of the wonderful properties of public-key encryption is that, so far as we know,[788] a third party's possession of Alice's public key and a complete description of the encryption algorithm puts that third party no closer to deducing Alice's private key or reading her messages than if the third party had the ciphertext alone. Thus, it is easy to establish a secure line of communication with anyone who is capable of implementing the algorithm. (In practice, this is anyone with a compatible decryption program or other device.) Sender and receiver no longer need a secure way to agree on a shared key. If Alice wishes to communicate with Bob, a new recipient with whom she has never communicated before, Alice and Bob can exchange the plaintext of their public keys or look each other up in a freely accessible directory of public keys. Then, Alice and Bob can each encrypt their outgoing messages with the other's public key and decrypt their received messages with their own secret private key.[789]

One drawback, however, is that public-key encryption and

Good Privacy is:

```
—BEGIN PGP PUBLIC KEY BLOCK—
Version: 2.6.2
mQCNAi4ztDUAAAEEAMjCVU3S9YJDTYD3f3XO1bZGCC0+zGLXrUE3ww0YwCktzp5r
OCR1sE4OxoL1GrECH9A/BVw0KAm7mpwb7n3wIg7TfasRmbDEKcc9jZfc9x1PpavD
TSXAx3a3Ab3R5PTJEl76EF2lU2jnVE7wo2GI1wZQuRDYFPWHwXpsXYZGTrN1AAUR
tC9NaWNoYWVsIEZyb29ta2luIDxtZnJvb21raUB1bWlhbWkuaXIubWlhbWkuZWR1
Pg==
=qpGN
—END PGP PUBLIC KEY BLOCK—
```

[788] *See* SCHNEIER, *supra* note 12, at 284-85 (stating that security of RSA evaporates if someone discovers a rapid means of factoring large numbers); *id.* at 318-20 (explaining that security of certain other public-key algorithms depends on the continuing inability of mathematicians to solve the long-standing problem of calculating discrete logarithms).

[789] Clearly, the security of the system evaporates if the private key is compromised, that is, transmitted to anyone.

decryption is much slower than commonly used single-key systems such as DES.[790] Thus, although public-key encryption is ideal for short messages, it is less than ideal for longer ones, and is particularly unsuitable for high-speed real-time applications like fast data transfer or telephone conversations. The speed problem can be overcome, however, by using a hybrid system. In a hybrid system, two parties who wish to communicate securely over an insecure medium use a public-key system to agree on a *session key* which then becomes the one-time key for a faster, conventional, relatively secure, single-key cipher such as DES.[791] Each time the parties initiate a new conversation, they generate a new session key, which, though lasting for the entire conversation, is never repeated.

If Alice and Bob are going to change their session key every time they talk so as to maximize the security of their single-key cipher, they need a secure means of agreeing on a session key each time they want to communicate. Ideally, the method would allow them to choose the session key in public, or on an insecure line, without fear of eavesdroppers. Public-key cryptography allows Alice and Bob to achieve this feat in either of two ways. Using the first method, Alice generates the session key, encrypts it with Bob's public key, and sends it to him. Bob decrypts the message with his private key, inputs the session key to his single-key software or telephone, and then the data exchange or conversation begins.[792] Alternatively, the parties can use Diffie-Hellman Key Exchange, in which Alice and Bob publicly send each other numbers from which they, and only they, can jointly calculate a session key. In Diffie-

---

[790] For example, RSA, one of the leading public-key programs, is at least 100 times slower than DES in software implementations, and up to 10,000 times slower in hardware. *See RSA Cryptography Today FAQ, supra* note 129, § 2.3.

[791] Another popular single-key cipher, which is not hampered by a 56-bit limit on key length, is called IDEA. *See* SCHNEIER, *supra* note 12, at 260-66.

[792] If Bob does not have a public key on record somewhere that Alice considers reliable, then Bob needs to authenticate it in a manner that protects against a "man in the middle" attack when he sends his public key to Alice. In a "man in the middle" attack, a third party intercepts Bob's first message. The man in the middle substitutes his public key for Bob's. Now Alice thinks she has Bob's key, and sends messages that are easily decrypted by the third party. The third party then reencrypts them with Bob's public key and sends them on to Bob who may never know the difference. A "man in the middle" attack will be prevented if Bob signs his public key with a digital signature that Alice can recognize. But this requires either that Bob register his public key for digital signatures somewhere trustworthy or that he find someone whose digital signature Alice already knows and who can affix a digital signature to Bob's transmission of his public key, thus attesting to the fact that it really comes from Bob.

Hellman Key Exchange, Alice and Bob agree on a number, b, which does not have to be secret, to use as the basis for their calculations. They also agree, again without any attempt at secrecy, on a large prime number which will serve as their modulus, m. (A modulus is the base for arithmetic operations. Usually we calculate in base ten; in binary arithmetic we calculate in base two. Alice and Bob will calculate using base m, where m is a large prime number.) Alice then selects a (secret) large random number A; Bob meanwhile selects a (secret) large random number B. Alice sends Bob a number she calculates as b^A (modulus m). Bob sends Alice a number he calculates as b^B (modulus m). Both Alice and Bob then compute b^{AB} (modulus m). This becomes their secret session key.

Diffie-Hellman works because it is computationally easy to calculate powers of numbers modulus m, but very, very difficult to find the logarithm of a large exponent of a number modulus m. Yet, this is what an eavesdropper would have to do to compute b^{AB} (modulus m) without knowing either A or B. Thus, if m is about 1000 bits long, Alice and Bob can do their calculations in seconds. At the current state of the art, however, the logarithmic computation would take a powerful computer a quintillion (a billion billion) years.[793]

Diffie-Hellman Key Exchange works for real-time communication because the parties can generate a session key at the start of the exchange, but it imposes potentially long delays on e-mail because the parties must exchange several messages to generate a session key before the parties can have a secure conversation. On the other hand, e-mail can be encrypted and decrypted at leisure, so the entire message can use public key encryption rather than just the session key. As a result, all that Bob needs in order to send Alice a secure e-mail is a reliable way of getting Alice's public key.

Key servers provide a simple way of making public keys generally available. Essentially, a key server is a computer with a white pages approach to public key management. Bob enters Alice's name and the key server replies with Alice's public key—if she has registered it. Key servers, whether run by the U.S. Post Office or

---

[793] *See* ACM REPORT, *supra* note 15, at 8 (noting that the logarithmic computation would "demand more than 2^{100} (or approximately 10^{30}) operations" and that "today's supercomputers . . . would take a billion billion years to perform this many operations"); SCHNEIER, *supra* note 12, at 275-77 (discussing Diffie-Hellman); *see also* Diffie & Hellman, *supra* note 784, at 644 (noting that in "a public key cryptosystem, enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible" (emphasis omitted)).

others, are likely to be an essential element of the National Information Infrastructure.

Key servers generally work on one of two principles: *the certification authority* or the *web of trust*. Under the certification authority paradigm, some central body authenticates the identity of the registrant when the key is first deposited. For example, the U.S. Post Office has proposed that it act as a certifying authority. Alice could then identify herself to the Post Office by providing identification similar to that currently required to get a passport. The Post Office would then add her key to its server, and/or provide Alice with a copy of her public key signed with the Post Office's private key.[794]

By contrast, there is no central authority for web-of-trust systems: Alice can upload a key to the key server at anytime. In order to demonstrate that the key purporting to be "Alice's" is hers, Alice must then find other persons to "sign" her key by uploading authentications signed with their private keys. Typically this is done by meeting face-to-face and exchanging public keys and showing identification. If Alice has her key signed by Carol, whom Bob knows or trusts, Bob can safely assume that the signature purporting to be from "Alice" is not in fact an impostor's. Suppose, however, that Alice and Bob do not have any friends in common, but that Bob's friend Carol has signed Ted's key, and Ted has signed Alice's key. From Bob's point of view this is not as good as if Carol, whom he knows, has signed Alice's key, but it is considerably better than nothing. Bob needs to decide how many intermediaries he is willing to accept before he considers a public key unreliable. The increase in the length of the chain of authentication can be offset by finding multiple routes to Alice. For example, Bob may still feel reasonably secure if he can establish three relatively long but independent chains of authentication.[795] This web-of-trust approach is the foundation of the PGP encryption system.[796]

---

[794] *See* OTA INFORMATION SECURITY, *supra* note 97, at 55-56. For a thorough survey of the legal and policy issues involved in setting up and running a certification authority, see generally MICHAEL BAUM, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES (1994).

[795] *See PGP™ User's Guide*, *supra* note 73.

[796] *See* GARFINKEL, *supra* note 73, at 235-36.

C. *Digital Signatures*

Verification of a message's origins takes on a new importance in the world of electronic mail, a world where all messages arrive on identical stationery in an identical typeface, having passed through many electronic hands en route. The fact that a message comes properly encrypted, even if the cipher is a simple one, tends to show that it was sent by the person who had access to the cipher and knew she was supposed to use it.[797] If the cipher is strong and the key tightly guarded, the use of the correct cipher strongly suggests that the message was sent by the person it purports to be from. Public-key systems in which a private key is held by only one person take this security feature to its logical extreme.

Public-key systems also allow users to append a so-called digital signature to an *unencrypted* message. A digital signature uniquely identifies the sender and connects the sender to the message. Because the signature uses the plaintext as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message.[798] A digital signature copied from one message has an infinitesimal chance of successfully authenticating any other message.[799]

The importance of a Digital Signature Standard (DSS), the prerequisite to a system of electronic commerce, has not been lost on the federal government. Nevertheless, for many years NIST was unable or unwilling to promote a standard. Although NIST had begun working on a DSS in the early 1980s, its progress was slowed by the close relation between digital signature and cryptographic systems: an algorithm that produces a secure digital signature can

---

[797] This is not irrefutable proof because a third party could obtain the key from the authorized user by stealth, purchase, accident, or torture (also known as "rubber hose cryptanalysis").

[798] Consider the following example: To sign a message, Alice does a computation involving both her private key and the message itself; the output is called the digital signature and is attached to the message, which is then sent. Bob, to verify the signature, does some computation involving the message, the purported signature, and Alice's public key. If the results properly hold in a simple mathematical relation, the signature is verified as genuine; otherwise, the signature may be fraudulent or the message altered, and they are discarded. *See RSA Cryptography Today FAQ*, *supra* note 129, § 2.13.

[799] *See* SCHNEIER, *supra* note 12, at 35 (noting that a digital signature using a 160-bit checksum has only a one in 2^{160} chance of misidentification).

also be used to produce a secure cipher. The U.S. government, however, wished to find a DSS which, although secure enough to be useful, nonetheless could not be used as an encryption system that the government might be powerless to break.[800] In August 1991, NIST announced its selection of the Digital Signature Algorithm (DSA) which, having been patented by an NSA employee, would be available royalty-free to all users.[801] NIST then encountered patent difficulties. These were exacerbated when a U.S. corporation acquired the rights to the main patent allegedly infringed by the DSA. In June 1993, NIST announced that it would give the corporation an exclusive license to the DSA; the U.S. government would have free use but everyone else would have to pay. Reaction from industry, which was already gravitating towards a competing corporation's product and was poised to accept NIST's standard only if it were royalty-free, was very negative.[802] In May 1994, NIST announced that it would not give an exclusive license to anyone, and that the DSA would be available royalty-free after all.[803] The alleged patent infringement was dealt with by the statement that NIST "has concluded there are no valid claims."[804] The DSS is now scheduled to be incorporated into Fortezza PCMCIA chips.

Meanwhile, academic cryptologists, ever vigilant for intentional weaknesses in government-sponsored cryptography, found an interesting property in the DSS proposed by NIST and approved by

---

[800] *See, e.g.*, Sherry L. Harowitz, *Building Security into Cyberspace*, SECURITY MGMT., June 1994, *available in* LEXIS, News Library, Curnws File (noting that the U.S. government "wants to discourage" the use of digital signatures other than the Clipper Chip for encryption purposes); Robert L. Hotz, *Sign on the Electronic Dotted Line*, L.A. TIMES, Oct. 19, 1993, at A1 ("Federal officials refused to adopt the earlier technique, called RSA, as a national standard because they were concerned that it could be used to conceal clandestine messages that could not be detected by law enforcement or national security agencies.").

[801] *See* A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), 56 Fed. Reg. 42,980, 42,980 (1991). The DSS was to be "applicable to all federal departments and agencies for the protection of unclassified information," and was "intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication." *Id.* at 42,981.

[802] *See* Kevin Power, *Use DSS with No Fear of Patent Liability, NIST Says*, GOV'T COMPUTER NEWS, Oct. 17, 1994, at 64 (noting overwhelming opposition to NIST's proposal to give a patent group an exclusive license to the Digital Signature Algorithm).

[803] *See* Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS), 59 Fed. Reg. 26,208, 26,209 (1994).

[804] *Id.*

the NSA. Small "subliminal" messages can be inserted into the digital signature without the signer's knowledge.[805] This property "allows an unscrupulous implementer of DSS to leak a [small] piece of the [user's] private key with each signature."[806] One commentator noted that the DSA "provides the most hospitable setting for subliminal communications discovered to date."[807] The NSA has not let on whether it knew about this feature when it agreed to the DSS.[808]

The proposed Capstone Chip combines the encryption functions of Clipper with the DSA.[809] It will be available in a PCMCIA card called Fortezza. Thus, if users wish to encrypt computer data transmissions with a government approved algorithm, they will have to take the DSA as part of the package.

Although digital signatures use strong cryptographic algorithms, they raise fewer, and different, policy issues from the Clipper Chip. The U.S. government is not concerned about the world-wide use of authentication software because affixing a signature to a plaintext message does not make that message any harder to read.[810] The real power struggle centers on whether the government will retain the capability to read private electronic messages and listen to private telephone conversations at will.

---

[805] A subliminal message is invisible to the user because it is encrypted and mixed in with the garbage-like stream of characters that constitutes the signature.

[806] SCHNEIER, *supra* note 12, at 313; *see also id.* at 390-92 (explaining how the subliminal channel works). The DSA is the algorithm used in DSS.

[807] Simmons, *supra* note 56, at 218.

[808] *See id.*

[809] *See Capstone Chip Technology*, *supra* note 16 (The Capstone Chip "implements the same cryptographic algorithm as the CLIPPER chip. In addition, the CAPSTONE Chip includes . . . the Digital Signature Algorithm (DSA) proposed by NIST . . . .").

[810] *See* ACM REPORT, *supra* note 15, at 3 (noting that "information that is authenticated and integrity-checked is not necessarily confidential; that is, confidentiality can be separated from integrity and authenticity").